

SYLLABUS

5 MAART - 5 MARS 2010

**Zolang er nog wat van
uw PRIVACY overblijft...**

Bescherming van privéleven en
persoonsgegevens tegen overheid en werkgever

**Tant qu'il vous reste
un peu de VIE PRIVEE...**

protection de la vie privée et des données
personnelles contre l'intrusion
des autorités et de l'employeur

WWW.PROGRESSLAW.NET

Met de steun van ELDH (European Association of Lawyers for Democracy and Human Rights) **en IADL** (International Association of Democratic Lawyers). Organisator vzw Dereac.

Avec le soutien de ELDH (European Association of Lawyers for Democracy and Human Rights) **et IADL** (International Association of Democratic Lawyers). En collaboration avec l'asbl Dereac.



ADVOCATEN | AVOCATS | LAWYERS

INLEIDING

Privacy, het recht op persoonlijke levenssfeer, de onschendbaarheid van woning en briefwisseling zijn fundamentele afweerrechten van de burgers tegen bemoeienissen van de overheid. Ook op de werkvloer zijn er grenzen aan het snuffelen in de privésfeer van de werknemer door de werkgever.

Iedere Belg zit gemiddeld in zo'n 300 databanken, van het rijksregister tot het e-health platform. Schiet er nog wel iets over van onze privacy? De nieuwe technologieën en het controleklimaat na 9/11 hebben dit 'heilig recht' zwaar onder druk gezet. George Orwell's Big Brother samenleving '1984' is vandaag geen fictie meer.

Het colloquium schetst een beeld van de privacy '2010'. Wordt artikel 8 van het EVRM nog wel gerespecteerd?

Er zijn wetten op de gegevensbescherming, maar wat betekenen die in de praktijk? Waar liggen de grenzen van de privacy in de arbeidsrelatie? Welke databanken registreren in België en Europa uw doen en laten en hoe zit het met de overdracht van gegevens van de ene naar de andere databank?

Op dit colloquium gaan we na met welke juridische middelen de privacy kan verdedigd worden. Wij doen dit aan de hand van de rechtspraak van het Europees Hof voor de Rechten van de Mens en van binnenlandse en buitenlandse ervaringen.

INTRODUCTION

La vie privée, l'inviolabilité du domicile et de la correspondance sont des droits fondamentaux des citoyens contre l'intrusion des autorités. Dans la sphère professionnelle, un employeur ne peut pas non plus s'immiscer sans limites dans la vie privée d'un employé.

Chaque Belge se retrouve en moyenne dans 300 banques de données, du registre national à la plateforme e-health. Que reste-t-il de notre vie privée? Les nouvelles technologies et le climat de contrôle que nous vivons depuis le 11 septembre 2001 ont réellement hypothéqué ce 'droit sacré'. La société Big Brother décrite par George Orwell dans '1984' n'est plus qu'une fiction.

Le colloque tente de faire le point de la situation sur la vie privée en 2010. L'article 8 de la CEDH est-il toujours respecté? Des lois concernant la protection des données existent, mais quel est leur impact dans la pratique? Quelles sont les limites de la vie privée dans une relation de travail? Quelles banques de données en Belgique et en Europe enregistrent vos faits et gestes et qu'en est-il du transfert des données d'une banque à une autre?

Ce colloque examinera aussi les moyens juridiques permettant de défendre notre vie privée, notamment à l'aide de la jurisprudence de la Cour européenne des Droits de l'Homme et d'expériences nationales et internationales.

INHOUDSTAFEL - TABLE DES MATIÈRES

Teksten van de sprekers - Textes des orateurs

1 Recht op privéleven versus controle en veiligheid **Droit à la vie privée contre contrôle et sécurité** **9**

La pression sur la vie privée et sur les autres droits et libertés fondamentales
Benoît VAN DER MEERSCHEN 9

Protection of personal data in the European Union + Powerpoint-presentation
Peter HUSTINX 13

Privacy opgeven in naam van veiligheid? Analyse van recente ontwikkelingen en gebruik van
nieuwe technologieën + Powerpoint-presentatie
Vertaling: Sacrifier le droit à la vie privée au nom de la sécurité? Analyse de développements
récents et de l'utilisation de nouvelles technologies
Raf JESPERS 33

2 Privacy in de arbeidsrelatie en op de werkvloer **La vie privée dans la relation de travail et sur le lieu de travail** **57**

De regelgeving bij aanwerving en tijdens de uitoefening van de arbeidsrelatie
Jos DUMORTIER 57

La jurisprudence belge et la jurisprudence de la Cour européenne des droits de l'homme
concernant la vie privée au travail
Steve GILSON..... 97

Expériences concrètes sur le lieu de travail
Manu GONZALEZ, Stephan GALON 99

Procedures and actions against LIDL, Siemens and other companies in Germany (+vertaling)
Dieter HUMMEL 101

3 Databanken en overdracht van persoonsgegevens

Banque de données et transfert de données individuelles

107

L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice: une affaire de balance ou une question de dignité?

Franck DUMORTIER 107

Erosion of privacy in the USA: from Bush to Obama

Mara VERHEYDEN-HILLIARD 139

De uitwisseling van persoonsgegevens in strafzaken tussen de EU-lidstaten en tussen de EU en de VS

Els DE BUSSEER 141

4 Juridische middelen en actiemogelijkheden voor de verdediging van de privacy

Quels moyens juridiques et quelles actions pour défendre la vie privée

155

Utilité et futilité des recours en matière de fichage par les services répressifs (+annexes)

Vertaling: Nut en beperkingen van de beroepen met betrekking tot de fichage van de burger door de politie (+bijlagen)

Mathieu BEYS 155

Procedures and actions in Germany, the UK, the Netherlands and France in connection with databases, legislation on hackers and data retention

Tony BUNYAN 229

5 Besluiten - Conclusions

Vanessa DE GREEF 235

LA PRESSION SUR LA VIE PRIVÉE ET SUR LES AUTRES DROITS ET LIBERTÉS FONDAMENTALES

Benoît Van der Meerschen



Protection de la vie privée et développement de nouvelles technologies: mission impossible?

Quel point commun entre un paiement par carte bancaire au supermarché, une réservation d'avion pour New York et la présence d'une puce sur votre carte d'identité électronique ? Votre vie privée est contrôlée !

Aujourd'hui en Belgique, chaque individu est fiché dans 600 banques de données différentes en moyenne. De nombreuses opérations quotidiennes laissent une trace électronique, les caméras de vidéosurveillance se multiplient, davantage de données d'un nombre croissant de personnes sont sauvegardées dans des fichiers, les pouvoirs intrusifs des services de police sont renforcés. Prises isolément, ces mesures peuvent paraître inoffensives mais, considérées globalement, elles représentent une indéniable atteinte au droit au respect de la vie privée, garanti entre autres par la Constitution et la Convention européenne des Droits de l'Homme.

A première vue, il peut paraître raisonnable de renoncer à une partie de son droit à la vie privée si cela peut permettre d'accroître le sentiment de sécurité (caméras de surveillance) ou de faciliter certaines activités humaines (paiement électronique, vote électronique). L'argument avancé pour défendre ce point de vue est le suivant: « Je n'ai rien à cacher, je n'ai donc rien à craindre de ces multiples violations de ma vie privée ». Sous-entendu : « Ceux qui critiquent ces mesures ont peut-être des choses à se reprocher ».

Or tout l'enjeu du droit à la vie privée est justement de ne pas avoir à se justifier sur celle-ci. De pouvoir se déplacer, rencontrer des gens, acheter, téléphoner ou envoyer un e-mail sans que ces données ne soient analysées, recoupées et utilisées. A de rares exceptions près, la plupart des nouvelles mesures portant atteinte à la vie privée sont prises au nom de la lutte contre l'insécurité physique, juridique ou politique. Qu'il s'agisse des banques de données ADN, des données biométriques, de la carte d'identité électronique, des systèmes de vidéosurveillance, des fichiers policiers ou du vote électronique, la « sécurisation » des relations humaines est avancée pour justifier leur utilisation.

Mais le coût de ces mesures est rarement mis en avant : une augmentation drastique du contrôle social. Contrôle des horaires, des déplacements et de la correspondance des travailleurs, dérives sécuritaires à l'occasion de la lutte contre le terrorisme, utilisation commerciale de certaines données, flou sur la

conservation et la protection d'autres données, les exemples ne manquent pas. Avec comme risque corollaire de ce contrôle, l'élaboration progressive de ce qui relève d'un comportement considéré comme « normal ». Et la sanction de tout comportement qui sort de cette norme. Exagération? Songez à cette alarme qui se déclenche dans le métro de Londres dès qu'une personne s'arrête de marcher plus de quelques secondes dans certains couloirs, où il n'y a rien et où il n'est donc pas « normal » de s'arrêter au milieu du flot des voyageurs.

Face à ces risques de dérives, il devient urgent que les citoyens soient informés et prennent conscience des conséquences de toutes ces mesures. Urgent également de préserver les espaces de liberté qui nous sont encore accordés et de refuser une société de surveillance permanente, cette surveillance ne touchant plus seulement l'« ennemi » (le terroriste, le voleur, le fraudeur, l'étranger) dont il faudrait se protéger, mais aussi et surtout nous-mêmes.

*Manuel Lambert
Conseiller juridique
Ligue des Droits de l'Homme*

Biographie sommaire

Benoît Van Der Meerschen est Secrétaire général d'Itéco depuis le 1er juin 2009 et Chargé de cours (Maître-assistant) en droit des étrangers à la Haute Ecole Paul-Henri Spaak depuis l'année académique 2000-2001

Il est licencié en droit, en droit international public et en droit public administratif de l'ULB.

Son expérience professionnelle étendue:

- *Juriste dans un syndicat, la Centrale générale des services publics (15 janvier 1993-15 juillet 1993),*
- *Juriste au Commissariat général aux réfugiés et aux apatrides (16 juillet 1993-30 juin 1994),*
- *Juriste à l'Auditorat du Conseil d'Etat (1er juillet 1994-31 octobre 1995),*
- *Responsable du service du contentieux de la commune d'Ixelles (1er novembre 1995-31 août 1996),*
- *Conseiller juridique-animateur à la Ligue belge francophone des droits de l'Homme (1er septembre 1996-31 mars 2002),*
- *Coordinateur de la Coordination des ONG pour les droits de l'Enfant (1er avril 2002-30 novembre 2002),*
- *Coordinateur de défense des Enfants international (DEI) (1er décembre 2002-31 décembre 2004),*
- *Assistant chargé d'exercices en Histoire du Droit et des institutions à l'Université Libre de Bruxelles (1993-2003),*
- *Chargé de cours (Maître-assistant) en droit international public et en droit européen à la Haute Ecole de Bruxelles (1998-2004),*
- *Secrétaire général du Centre national de Coopération au Développement (CNCD-11.11.11.) (1er avril 2005 au 31 mars 2008),*
- *Délégué au CAL (1er mai 2008 au 7 mai 2009),*

Il a entrepris fréquentes mission pour le compte de la Fédération internationale des Ligues des droits de l'Homme, la Francophonie, la Communauté française et l'ccco dans différents pays : Congo-Brazzaville, RDC, Rwanda, Sénégal, Gambie, Mali, Burkina Faso, Togo, Tchad, Cameroun, Tunisie, Liban et Haïti.

Il est aussi actif dans plusieurs associations de défense :

- *des droits de l'Homme,*
- *du droit des étrangers,*
- *du droit de la jeunesse,*
- *de solidarité internationale.*

Publications diverses

- *Plusieurs publications dans le Journal du Droit des Jeunes, la Chronique de la LDH, La Lettre de la FIDH, résistances, Imagine, la Revue Nouvelle, la Nouvelle Tribune, Le Soir, la Libre Belgique, l'Echo...*
- *Belgique, terre d'écueils, en collaboration avec Dan Van Raemdonck, Labor, 2001.*

PROTECTION OF PERSONAL DATA IN THE EUROPEAN UNION

Peter Hustinx

Peter Hustinx and Giovanni Buttarelli are members of the institution. They took office on 17 January 2009. As members, elected by the European Parliament and the Council, they have a different status to that of the staff of their secretariat. Read more about their appointment and previous experiences.

The EDPS' general objective is to ensure that the EC institutions and bodies respect the right to privacy when they process personal data and develop new policies. A number of specific duties of the EDPS are laid down in Regulation (EC) No 45/2001. The three main fields of work are:

Supervision

One of the EDPS' main tasks is to supervise personal data processing by the European institutions and bodies. This supervision work takes various forms.

The bulk of it is based on notifications of processing operations presenting specific risks. These need to be **prior checked** by the EDPS. Based on the facts submitted to him, the EDPS will examine the processing of personal data in relation to Regulation (EC) No 45/2001. In most cases, this exercise leads to a set of recommendations that the institution or body need to implement so as to ensure compliance with data protection rules.

The EDPS receives **complaints** from EU staff members as well as from other people who feel that their personal data have been mishandled by a European institution or body. If a complaint is admissible, the EDPS usually carries out an inquiry. The findings are communicated to the complainant, and necessary measures are adopted.

The EDPS may adopt opinions on **administrative measures** related to data protection adopted by European institutions and bodies.

The EDPS may carry out **inquiries** on his own initiative. Inquiries and **inspections** are essential for a supervisory authority to have the means for fact-finding, following up of cases and monitoring of compliance in general.

In order to monitor compliance with Regulation (EC) No 45/2001, the EDPS largely relies on the **Data Protection Officers** (DPOs) who are to be appointed in each institution/body. Apart from bilateral meetings and contacts with the DPOs, the EDPS also takes part in the regular meetings of the DPO network.

Since January 2004, the EDPS has ensured the supervision of the central unit of Eurodac. An essential aspect of this supervision is the cooperation with national supervisory authorities and the drawing up recommendations for common solutions to existing problems.

The EDPS publishes **thematic guidelines** on critical issues to serve as reference documents for the European administration.

Consultation

The **EDPS advises** the EU institutions and bodies on data protection issues in a range of policy areas. His consultative role relates to proposals for **new legislation** as well as **soft law** instruments like communications that affect personal data protection in the EU. He also monitors **new technologies** that may have an impact on data protection. The objective is to ensure that the EU citizens' fundamental rights to protection of privacy and personal data are maintained, while society evolves.

One of the primary tasks of the EDPS is to **examine the data protection and privacy impact** of proposed new legislation. The Policy paper of 2005 elaborates how this role is interpreted in terms of limitations in scope, working methods and main orientations. The EDPS uses different instruments in order to exercise this role.

The first instrument is a **planning tool**. Each year in December, the EDPS publishes an **inventory** of his priorities for the coming year. It lists the most relevant Commission proposals, which may require a formal reaction by the EDPS. Those proposals that are expected to have a strong impact on data protection are given high priority. This may also apply to research projects.

The second and most important instrument is the formal public **opinion**. By issuing opinions on a regular basis, the EDPS establishes a consistent policy on data protection issues. The opinions are addressed to those involved in the legislative negotiations, but also published on the website as well as on the Official Journal of the EU.

A third instrument of intervention is the EDPS **comments**, which address data protection issues for instance in Commission communications.

A final instrument is the possibility to **intervene** in cases before the **Court of Justice**, the Court of First Instance and the Civil Service Tribunal.

Cooperation

The third leg of EDPS' activities can best be described as cooperation. It covers work on specific issues, as well as more structural collaboration together with other data protection authorities. This may involve issues which have an impact on how to interpret a provision of Directive 95/46, which has been implemented into national laws. It can also be relevant in cases where similar complaints have been launched in several Member States. The overriding aim of the EDPS is to promote consistency in the protection of personal data.

The central forum for cooperation in the EU is the **Article 29 Working Party**. This is where the national data protection authorities meet to exchange views on current issues, to discuss a common interpretation of data protection legislation and to give expert advice to the European Commission.

The EDPS also participates in the work to ensure good data protection in the **EU's third pillar**, which covers police and judicial cooperation. This includes attending a number of meetings of the Joint Supervisory Bodies of the third pillar information systems. He is also a member of the Working Party on Police set up by the European Conference to prepare advice in third pillar matters. In addition, the EDPS has also taken part in meetings of the Joint Supervisory Authority of the Schengen Information System, which falls under both the first and third pillars of the EU.

One of the most important cooperative tasks relates to **Eurodac**, where the responsibilities for data protection supervision are shared. Eurodac is a large scale IT system which contains digital fingerprints of asylum seekers. It consists of national units (subject to national law), and a central unit (subject to Regulation 45/2001). A coordinated approach is essential, as supervision depends on collaboration between the national data protection authorities and the EDPS. The EDPS therefore organises biannual coordination meetings.

Two major data protection conferences are organised each year. Every spring, a **European Conference** assembles data protection officials from authorities in the Member States of the EU and the Council of Europe. And every autumn, a wide range of data protection experts, from the public as well as the private sector, gather for the International Conference.

International organisations which are exempted from national law, often find themselves without a legal framework for data protection. Because virtually all of them process personal data, the EDPS decided to organise a workshop on 'data protection as part of good governance in international organisations' with representatives from some 20 organisations. A follow-up workshop is being prepared.

ANNUAL REPORT 2008 — EXECUTIVE SUMMARY

Introduction

This is the Executive Summary of the Annual Report 2008 of the European Data Protection Supervisor (EDPS). This Report covers 2008 as the fourth full year of activity of the EDPS as a new independent supervisory authority. This report also concludes the first EDPS mandate and provides an opportunity to take stock of developments since the start.

Peter Hustinx (Supervisor) and Joaquín Bayo Delgado (Assistant Supervisor) took office in January 2004 to set up the authority which deals with the protection of personal data at the level of the European Union (EU). The mission of the EDPS is to ensure that the fundamental rights and freedoms of natural persons, and in particular their privacy, with regard to the processing of personal data are respected by the Community institutions and bodies.

As laid down in Regulation (EC) No 45/2001¹, the EDPS' main activities are to:

- monitor and ensure that the provisions of the Regulation are complied with when Community institutions and bodies process personal data (supervision);
- advise the Community institutions and bodies on all matters relating to the processing of personal data. This includes consultation on proposals for legislation and monitoring new developments that have an impact on the protection of personal data (consultation);
- cooperate with national supervisory authorities and supervisory bodies in the "third pillar" of the EU with a view to improving consistency in the protection of personal data (cooperation).

This report shows that great progress was achieved both in supervision and in consultation. Compliance with data protection rules and principles in Community institutions and bodies is developing, but there are still great challenges ahead. The emphasis of supervision is therefore shifting to monitoring the implementation of recommendations in prior checking and to improving the level of compliance in agencies. In this context, the EDPS has also completed a first series of on the spot inspections in different institutions and bodies to measure compliance in practice.

The EDPS further improved his performance in consultation in 2008 and submitted opinions on an increasing number of proposals for legislation. He widened the scope of his interventions to a greater variety of policy areas, and to all stages of the legislative procedure. The majority of the EDPS opinions continued to concern issues related to the area of freedom, security and justice, but other policy areas, such as e-privacy, public access to documents and cross-border healthcare, were also quite prominent.

¹ Regulation (EC) No. 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001.

Cooperation with national supervisory authorities continued to focus on the role of the Article 29 Data Protection Working Party, which resulted in the adoption of a new work programme and several good results in its first year of operation. The EDPS also continued to put emphasis on the coordinated supervision of Eurodac and to cooperate closely with data protection authorities in the area of police and judicial cooperation.

Results in 2008

The Annual Report 2007 mentioned that the following main objectives had been selected for 2008. Most of these objectives have been fully or partially realised.

- **Support of data protection officers' network**

The EDPS continued to give strong support to data protection officers and encouraged a further exchange of expertise and best practices among them. Particular attention was given to data protection officers of recently established agencies.

- **Role of prior checking**

A record number of prior checking opinions were issued, with still some work ahead to finish prior checking of existing processing operations for most institutions and bodies. More emphasis was put on the implementation of recommendations.

- **Horizontal guidance**

Guidance on relevant issues common to most institutions and bodies (e.g. recruitment of staff, processing of health related data) was developed, at first to facilitate prior checking for agencies. This guidance will soon be made available for all interested parties.

- **Measuring compliance**

The EDPS continued to measure compliance with Regulation (EC) No 45/2001 by all institutions and bodies, and will report on progress made by mid 2009. In addition to this general survey, a first series of inspections was held in different institutions and bodies to verify compliance on specific issues.

- **Large scale systems**

The EDPS has continued to develop a coordinated supervision of Eurodac together with national supervisory authorities, and to implement the work programme adopted for this purpose. The EDPS has also made first steps with regard to other large scale systems, such as SIS II and VIS.

- **Opinions on legislation**

The EDPS issued a record number of opinions or comments on proposals for new legislation or related documents, covering a wider area than ever before, and ensured adequate input from the first until the last phase of the legislative procedure.

- **Treaty of Lisbon**

The impact of the Lisbon Treaty has been closely analyzed, but its entry into force depends on final ratifications by a few Member States. The analysis highlighted that the Treaty has a great potential impact, both for institutional and substantive reasons, with clear opportunities for improvement of data protection.

- **On line information**

The information available on the EDPS website has been improved, both by updating and developing its content, and by enhancing its accessibility. Further improvements are expected in the course of 2009, and will also include the electronic newsletter.

- **Rules of procedure**

The preparation of rules of procedure, covering the different roles and activities of the EDPS, has made good progress, together with the development of internal case manuals for the most important activities. The results will be available on the EDPS website in the course of 2009 with practical tools for interested parties.

- **Resource management**

The management of financial and human resources was consolidated or further developed and other internal processes were enhanced. The functionality and efficiency of internal control functions were also improved.

Objectives for 2009

This will be the first year of a new EDPS mandate, with a partly new composition of the institution. A mixture of continuity and change is therefore to be expected. This year will be used for a strategic assessment of the roles and tasks of the EDPS and to set out main lines of development for the next four years. This reflection will coincide with significant changes in the EDPS external environment, such as the challenges coming from a new European legislature, a new European Commission, a possible entry into force of the Lisbon Treaty, other new long term policies and frameworks and their combined impact on data protection. The EDPS intends to take a clear position in this context and will report on conclusions in the next Annual Report.

The following main objectives have been selected for 2009, without prejudicing the outcome of this strategic reflection. The results achieved will also be reported next year.

- **Support of data protection officers' network**

The EDPS will continue to give strong support to data protection officers, particularly in recently established agencies, and encourage an exchange of expertise and best practices among them, in order to strengthen their effectiveness.

- **Role of prior checking**

The EDPS intends to complete prior checking of existing processing operations for most institutions and bodies, and put increasing emphasis on the implementation of recommendations. Prior checking of processing operations common to most agencies will receive special attention.

- **Horizontal guidance**

The EDPS will continue to develop guidance on relevant issues common to most institutions and bodies, and make it generally available. Guidelines will be published on video-surveillance that will also help to focus attention to situations giving rise to specific risks.

- **Complaint handling**

The EDPS will publish a policy framework for the handling of complaints to inform all parties involved about relevant procedures, including criteria on whether or not to open an investigation on complaints presented to him.

- **Inspection policy**

The EDPS will continue to measure compliance with Regulation (EC) No 45/2001, with different kinds of checks for all institutions and bodies, and increasingly execute inspections on the spot. A general inspection policy will be published on the EDPS website in 2009.

- **Scope of consultation**

The EDPS will continue to issue timely opinions or comments on proposals for new legislation, on the basis of a systematic inventory of relevant subjects and priorities, and ensure adequate follow up.

- **Stockholm program**

The EDPS intends to give special attention to the preparation of a new five-year policy programme for the area of freedom, security and justice, for adoption by the European Council at the end of 2009. The need for effective safeguards for data protection will be emphasized as a key condition.

- **Information activities**

The EDPS will further improve the quality and effectiveness of the online information tools (website and electronic newsletter) and will assess and where necessary update other information activities.

- **Rules of procedure**

The EDPS will adopt and publish rules of procedure, confirming or clarifying present practices as to his different roles and activities. Practical tools for interested parties will be made available on the website.

• Resource management

The EDPS will consolidate and further develop activities relating to financial and human resources, and enhance other internal work processes. Special attention will be given to the long term recruitment of staff, the need for additional office space, and the development of a case management system.

Supervision

One of the main roles of the EDPS is to supervise in an independent manner processing operations carried out by Community institutions or bodies. The legal framework is Regulation (EC) No 45/2000, which establishes a number of obligations for those who process data, along with a number of rights for those whose personal data are processed.

Processing operations of personal data that do not present special risks for the data subjects are notified only to the data protection officer of the institution or body concerned. When personal data processing presents special risks for those whose data are processed, it needs to be prior checked by the EDPS. The EDPS then determines whether or not the processing complies with the Regulation.

The supervisory tasks, overseen by the Assistant Supervisor, range from providing advice and assisting data protection officers, through prior checking risky processing operations, to conducting inquiries, including on the spot inspections, and handling complaints.

Prior checks

In 2008, prior checking continued to be the main aspect of the EDPS in his supervisory role.

As mentioned in previous annual reports, the EDPS has constantly encouraged data protection officers to increase the number of prior checking notifications to the EDPS. The deadline of spring 2007 for receipt of notifications to be prior checked by the EDPS – ex post cases – was fixed to trigger Community institutions and bodies to increase their efforts towards a complete fulfilment of their notification obligation. The effect was a significant increase of notifications.

Overall, 2008 was an intensive year of work, with more prior check opinions (105 opinions) issued than in any of the preceding years. Only a limited number of those cases (18 cases) were “proper” prior checking cases, i.e. the institutions concerned followed the procedure involved for prior checking before implementing the processing operation.

For the first time, the EDPS decided to suggest the withdrawal of some notifications. This was due to the fact that those notifications either concerned old processing operations about to be substituted by new ones or notifications that lacked sufficient information rendering it impossible to treat them with a correct understanding of the facts or the procedure.

As regards timelines, the number of days needed by the EDPS to draft opinions represents a decrease of more than two days of work compared to 2007. It is a very satisfactory figure

considering the increase of numbers and complexity of the notifications. The EDPS is however concerned about the lengthy periods needed by the institutions and bodies to complete information. In this context, he once again reminds them of their obligation to cooperate with the EDPS and to provide him with the requested information.

In 2008, the ex-post prior checks cases² mainly covered the following issues: health related data processed by institutions and bodies, recruitment of staff and selection of candidates, staff evaluation, journalist accreditation, identity management systems, access control and security investigations.

As regards main issues in proper prior-checks, these concerned specific selection procedures, notably at the Fundamental Rights Agency and for the EDPS, a pilot project concerning individual monitoring, real time, identity and access control, as well as e-monitoring.

Some meaningful issues have also been addressed for the first time, including identity management service, access control with iris scanning or fingerprint authentication, security investigations, monitoring of the use of the Internet by staff, and CCTV system.

Complaints

The total number of complaints continued to increase in 2008 (91 complaints received), with less admissible complaints than before (23 admissible complaints), but more complexity on the whole. A large majority of complaints were declared inadmissible in particular because they exclusively concerned processing of personal data on the level of the Member States (where national data protection authorities are competent). Admissible cases related in particular to issues such as access to data, processing of sensitive data, right of rectification and obligation to provide information.

The EDPS has continued working on a policy framework for the handling of complaints. The main elements of the procedure and a model form for the submission of complaints, together with information on the admissibility of complaints, will be made available on the EDPS website in 2009. This publication is expected to help potential complainants submit a complaint, whilst limiting the number of clearly inadmissible complaints.

Inspection policy

In the framework of the "Spring 2007 deadline", the first part of the operation launched in 2007 took the form of letters addressed to directors of institutions and agencies in order to measure the level of compliance with the Regulation. On the basis of the feedback received, the EDPS drafted a general report, which was made public in May 2008 and was sent to all institutions and agencies. As announced, the operation was the start of an ongoing exercise by the EDPS to ensure compliance with the Regulation, leading to possible on-the-spot inspections.

² "Ex post" prior checks relate to processing operations that started before the appointment of the EDPS and the Assistant Supervisor (17 January 2004), and that therefore could not be checked prior to their start.

In this context, the EDPS has further developed his inspection policy and has completed a first series of on the site inspections in different institutions and bodies to measure compliance in practice. Inspections can be triggered by a complaint or can be carried out at the EDPS' own initiative. During inspections, the EDPS verifies facts and reality on the spot. Inspections can also largely contribute to raise awareness for data protection matters in the inspected institutions.

In 2008, the EDPS defined the first comprehensive procedure for his inspection activities. It consisted in a three-phase process:

- in the first phase, two rehearsal visits were carried out to test the EDPS methodology on site;
- in the second phase, the EDPS refined its practical methodology;
- in the third phase, two inspections were carried out in European institutions and bodies – the European Economic and Social Committee and the European Food Safety Authority – which were selected in the framework of the spring 2007 exercise.

Administrative measures

The EDPS also continued to provide advice on administrative measures envisaged by Community institutions and bodies in relation to the processing of personal data. A variety of challenging issues was raised, including a new model of medical certificate; access to public documents containing personal data; applicable law to certain processing activities; transfer to a national tribunal of a medical file; implementing rules of Regulation (EC) No 45/2001 and complaints handled by the European Ombudsman.

Video-surveillance

The EDPS continued to work on his video-surveillance guidelines to provide practical guidance to EU institutions and bodies on compliance with data protection rules when using videosurveillance systems. The first internal working draft of the guidelines was prepared by the end of 2008. The draft will be made public for consultation by mid-2009.

Consultation

The EDPS advises the Community institutions and bodies on data protection issues in a range of policy areas. This consultative role relates to proposals for new legislation as well as other initiatives that may affect personal data protection in the EU. It usually takes the shape of a formal opinion, but the EDPS may also provide guidance in the form of comments or policy papers. Technological developments having an impact on data protection are also monitored as part of this activity.

EDPS opinions and key issues

The EDPS issued **14 opinions** on proposed EU legislation in 2008. As in previous years, a substantial part of the opinions relate to the area of **freedom, security and justice**, both in the Community “pillar” and in the field of police and judicial cooperation in criminal matters (“third pillar”). This area represents almost half of the legislative opinions issued, namely six out of 14. An important development in this area was the adoption of the **Data Protection Framework Decision** of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Throughout the negotiations, this piece of legislation has been a major focus of attention for the EDPS who issued three opinions as well as comments on the subject.

The proposal to modify the Regulation on **public access to documents** held by EU institutions as well as the review of the Directive on privacy and electronic communications (**ePrivacy Directive**) were also of special attention to the EDPS. **Passenger Name Records (PNR)** related matters were quite prominent as well in the EDPS consultative activities, in particular with regard to the follow up of the EU PNR proposal.

Exchange of information

The issue of exchange of information, in particular the establishment of information systems and access to those systems, was a key focus area. The EDPS adopted opinions on information exchange systems that were proposed in the framework of the Internal Market Information System (IMI), Eurojust, road safety, the protection of children using the Internet, ECRIS, the EU-US High Level Contact Group on information sharing, and the European e-Justice strategy. Preliminary comments were also issued on the Commission’s EU border management package.

The EDPS opinions emphasised the need for such exchange of information to be properly and carefully assessed in each case. Moreover, when such exchange of information is established, specific data protection safeguards need to be implemented.

New technologies

On several occasions, the EDPS addressed the issue of the use of new technologies (e.g. ECRIS, European e-Justice strategy). He repeatedly called for ensuring that data protection considerations are taken into account at the earliest possible stage (“**privacy-by-design**”). He also highlighted that technology tools should be used not only to ensure the exchange of information, but also to enhance the rights of the persons concerned.

The developments taking place in the **Information Society** have again been closely followed and commented upon, such as RFID and ambient intelligence, as a follow up to the European Commission’s Communication on **RFID** and the related EDPS opinion.

The EDPS also clarified his possible contributions to the **EU research and technological development** (RTD) and consolidated actions already initiated. A **policy paper** was adopted to describe the possible role the institution could play for research and developments projects in the seventh framework programme for RTD.

Quality of data

Quality of data was another important theme. A high level of accuracy of data is indeed needed to avoid ambiguity concerning the content of information processed. It is therefore imperative that the accuracy be regularly and properly checked. Moreover, a high level of data quality represents not only a basic guarantee for the data subject, but also facilitates the efficient use for those who process the data.

New developments and priorities

A number of perspectives for future changes, which will serve as the agenda of main priorities for the EDPS, have been identified. They include new **technological trends** raising critical data protection and privacy concerns, such as the development of cloud computing systems³ and light-speed DNA sequencing technology.

As regards new developments in **policy and legislation**, the main issues to which the EDPS intends to devote special attention include the following:

- reflection on further improvements of the **Data Protection Framework Decision** to increase the level of protection provided by the new instrument in the third pillar;
- the future of the Data Protection Directive;
- the European Commission's multi-annual program in the area of freedom, security and justice - referred to as "Stockholm Program";
- major trends in law enforcement and legislative activities relating to the fight against terrorism and organised crime;
- the revision of the Regulation on public access to documents;
- new initiatives aimed at enhancing cross-border healthcare in combination with the use of information technologies.

Cooperation

The EDPS cooperates with other data protection authorities in order to promote consistent data protection throughout Europe. This cooperative role also extends to cooperation with supervisory bodies established under the EU third pillar and in the context of large scale IT systems.

³ Cloud computing refers to the use of Internet ("cloud") based computer technology for a variety of services. It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet.

The main platform for cooperation between data protection authorities in Europe is the **Article 29 Working Party**, which provides the European Commission with independent advice on data protection matters. The EDPS participates in the activities of the Working Party, which plays a crucial role in the uniform application of the Data Protection Directive.

The EDPS and the Working Party have cooperated in good synergy on a range of subjects, but especially focussing on the implementation of the Data Protection Directive and on data protection challenges raised by new technologies. The EDPS also strongly supported initiatives taken to facilitate international data flows (e.g. Binding Corporate Rules).

In 2008, the Working Party adopted opinions on proposals for legislation, which in some cases had also been subject to EDPS opinions (e.g. review of ePrivacy Directive). While consultation of the EDPS is a compulsory feature of the EU legislative process, contributions of the Working Party are also very useful, particularly since they may contain special points of attention from a national perspective. The EDPS therefore welcomes these contributions which have been consistent with his own opinions.

One of the most important cooperative tasks of the EDPS relates to the coordinated supervision of **Eurodac**, where the responsibilities for data protection supervision are shared between the national data protection authorities and the EDPS. The Eurodac Supervision Coordination Group – composed of national data protection authorities and the EDPS – met twice in 2008 and focused on the implementation of the work programme adopted by the Group in December 2007. Three topics had been selected within the work program for closer examination and reporting, namely: information of the data subjects, children and Eurodac, and DubliNet⁴. At the same time, the framework in which the Group is operating has also attracted attention: the European Commission has undertaken the review of the Dublin and Eurodac Regulations, in the framework of the asylum measures in general.

The need for close cooperation between the EDPS and other data protection authorities in **third pillar matters** – area of police and judicial cooperation - has become more apparent in recent years through the increase of initiatives at European and international levels aimed at collecting and sharing personal data. The EDPS strives to ensure a high and consistent level of data protection in the fields of the supervisory data protection bodies (Joint Supervisory Bodies for Schengen, Europol, Eurojust and the Customs Information System) established under the EU third pillar. In 2008, the EDPS actively contributed to the meetings held by the Working Party on Police and Justice that addressed sensitive issues, such as the implementation of the Prüm Treaty, the Framework Decision of Data Protection in the third pillar and PNR.

Cooperation in other **international fora** continued to attract attention. As in previous years, the EDPS took part in the European and International Conferences of Data Protection and Privacy Commissioners, which gave participants the opportunity to discuss topical challenges for data protection, such as developments related to security and new technologies and the issue of privacy in a borderless world. Appropriate follow-up was also given to the “London initiative” on raising awareness of data protection and making it more effective. Finally, following similar events organised in 2005 and 2007, a third workshop on data protection in international organisations is under consideration.

⁴ DubliNet is the secure electronic network of transmission channels between the national authorities dealing with asylum applications. Usually, a “hit” in the Eurodac system will trigger an exchange of data about the asylum seeker. This exchange will use DubliNet.

Communication

Information and communication play a pivotal role in ensuring visibility of the EDPS' main activities and in raising awareness both of the EDPS' work and of data protection in general. This is all the more strategic since the EDPS is still a relatively new institution and awareness of its role at EU level therefore needs to be further consolidated.

Four years after the start of work, we can see that the emphasis placed on communication generated payoff in terms of **visibility**. Meaningful indicators of achievements include a higher volume of requests for information, increased traffic on the website, a constant rise in the number of subscribers to the newsletter, regular requests for study visits at the EDPS and invitations to speak at conferences. In addition, more systematic contact with the media and, as a result, substantial rise in media coverage of EDPS activities further emphasize the view that the EDPS has become a point of reference for data protection issues.

Media relations continued to be a key focus of communication activities, with the EDPS giving about twenty-five **interviews** to journalists from the print, broadcast and electronic media in 2008. The press service issued 13 **press releases**, most of which related to new legislative opinions having a high public general relevance. They covered issues such as the review of the ePrivacy Directive, adoption of the Framework Decision on Data Protection in the third pillar, public access to EU documents, and transatlantic information sharing for enforcement purposes. A press conference was also organised in May 2008 to present the main conclusions of the Annual Report 2007 to the press.

In addition to media enquiries received on a regular basis, the press service dealt with about 180 public **requests for information** coming from a wide range of individuals and stakeholders. The EDPS welcomed visits from **student groups** specialised in European law, data protection and/or IT security issues to also reach out to the academic world.

With a view to giving further visibility to his ongoing activities, the EDPS continued to make use of the following other information tools:

- website: technical upgrades and content improvements, including the development of a "Glossary of terms" on the protection of personal data and a "Questions and Answers" section, were brought to the website. Statistical data show that, from 1 February to 31 December 2008, the website received a total of 81 841 visitors, with a peak of 10 095 visitors in May at the time of the publication of the Annual Report 2007;
- electronic newsletter: five issues of the EDPS newsletter were published in 2008. The number of subscribers rose significantly between 2007 and 2008. Preparatory work was undertaken to provide an upgraded newsletter with the aim of providing a more reader-friendly information tool;
- promotional events: the EDPS renewed his participation at the Data Protection Day and the EU Open Day; holding information stands in the main EU institutions;
- information brochure: the development of an updated information brochure was initiated, notably in view of the first EDPS mandate coming to an end in January 2009.

Administration, budget and staff

With the aim of further consolidating its positive start and, consequently, handling new tasks assigned, **additional resources** both in terms of budget (increasing from EUR 4 955 726 in 2007 to EUR 5 307 753 in 2008) and staff (from 29 to 33) have been attributed to the EDPS.

As regards the **budget**, a new budget terminology was applied in 2008 so as to ensure the transparency required by the budgetary authority. In its report on the 2007 financial year, the European Court of Auditors stated that the audit had not given rise to any observations.

In terms of **human resources**, the growing visibility of the institution is leading to an increased workload, together with an expansion of tasks. The EDPS has however chosen to use controlled growth to ensure that new staff members are fully taken on board. The EDPS therefore called for the creation of only four posts in 2008. The traineeship programme continued to host about two trainees per session. In addition, two seconded national experts from national data protection authorities were recruited.

As regards the EDPS's **organisation chart**, the increasing workload has prompted the creation of a new function as coordinator. To this end, five coordinators have been designated in the consultation and supervision teams.

With regards to **internal control**, the evaluation performed by the EDPS services and the Internal Auditor have demonstrated the functionality and efficiency of the internal control system and its ability to provide reasonable assurance for the achievement of the institution's objectives.

The EDPS has appointed his own **Data Protection Officer** to ensure the internal application of the provisions of Regulation (EC) No 45/2001. The process to identify processing operations containing personal data and to determine which operations are subject to prior checking continued in 2008. An inventory of internal operations has been finalised. On this basis, the first notification process has been launched.

New **internal rules** necessary for the proper functioning of the institution were adopted, including decisions on certification, on security measures and on the appointment of a local security officer for EDPS.

The implementation of a new **document management** system (GEDA) has been followed through. This implementation is seen as a first step in the development of a case flow management system for improved support to EDPS activities.

POWERPOINT PRESENTATION



European Data Protection Supervisor

Protection of personal data in the European Union

Peter Hustinx
5 March 2010

PROGRESS Lawyers Network, Brussels, 5 March 2010




European Data Protection Supervisor

EU Data Protection

- Art 8 ECHR: private life
- CoE Convention 108
 - *Personal data > basic principles*
- Directives 95/46 and 2002/58
 - *National laws of MS*
- Regulation (EC) 45/2001
 - *EU institutions and bodies*
- Art 7-8 Charter > Lisbon Treaty

PROGRESS Lawyers Network, Brussels, 5 March 2010



European Data Protection Supervisor

Article 8 EU Charter

1. Everyone has the right to the protection of personal data concerning him or her (> Art. 16 TFEU).
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

PROGRESS Lawyers Network, Brussels, 5 March 2010

Role of EDPS

- Supervision
 - Monitoring and ensuring compliance > DPO
 - » *prior checks, consultations, guidelines, complaints, inquiries, inspections, etc*
- Consultation
 - Advising on new legislation, court interventions, monitoring technology, R&D
- Cooperation
 - WP29, JSA, EUODAC, VIS, national DPAs

PROGRESS Lawyers Network, Brussels, 5 March 2010

Supervision

- Prior checking & Guidelines
 - Staff recruitment, health data at work, e-monitoring, video-surveillance
- Complaints & Inquiries
 - Scope: EU staff + interested persons
 - Structured approach: preliminary examination, further inquiries, investigations at own initiative
- Monitoring & Inspections
 - “Spring” exercises and follow up

PROGRESS Lawyers Network, Brussels, 5 March 2010

Consultation

- Legislation & Policy
 - Proactive: inventory, priorities, impact
 - Structured approach: informal comments, public opinions or comments, follow up
- General frameworks
 - Directive 95/46, e-Privacy, Police & Justice
- Specific issues
 - Asylum, public access, e-health, e-transport, biometrics, terrorist lists, transatlantic data, taxation, organ donation, pharmacovigilance

PROGRESS Lawyers Network, Brussels, 5 March 2010

Court interventions

- PNR > Community data protection
 - All relevant, except preliminary procedures
- Clarifying data protection perspective
 - Including relation with public access
 - Legal base of Data Retention Directive
 - Data Protection Authorities' independence
 - Access to information on competitions
- Pleadings on EDPS website

PROGRESS Lawyers Network, Brussels, 5 March 2010

WP29: "Future of Privacy"

- Comprehensive framework
 - » More effectiveness
 - » Privacy by design
- Controllers' responsibility
 - » More accountability
- Empowering data subjects
 - » Exercising choice
- More effective supervision
 - » Enforcement powers

PROGRESS Lawyers Network, Brussels, 5 March 2010

More information:

www.edps.europa.eu
edps@edps.europa.eu

Postal address:
Rue Wiertz 60 - MO 63
B-1047 Brussels

PROGRESS Lawyers Network, Brussels, 5 March 2010

Brief biography

Peter J. Hustinx (1945) has been European Data Protection Supervisor since January 2004 and was re-appointed by the European Parliament and the Council in January 2009 for a second term of five years.

He has been closely involved in the development of data protection legislation from the start, both at national and at international level.

Before entering his office, Mr. Hustinx was President of the Dutch Data Protection Authority since 1991. From 1996 until 2000 he was Chairman of the Article 29 Working Party.

He received law degrees in Nijmegen, the Netherlands, and in Ann Arbor, USA. Since 1986 he has been deputy judge in the Court of Appeal in Amsterdam.

PRIVACY OPGEVEN IN NAAM VAN VEILIGHEID? ANALYSE VAN RECENTE ONTWIKKELINGEN EN GEBRUIK VAN NIEUWE TECHNOLOGIEËN.

Raf Jespers

*Dames en Heren,
Beste Collega's,*

U bent vandaag al door een tiental camera's gefilmd. Sommigen onder jullie werden al van op afstand geïdentificeerd wanneer ze om naar hier te komen hun Mobib-pas met RFID-chip (Radio Frequency Identificatie) gebruikten in de Brusselse metro. Van de facebook gebruikers onder jullie is het in hun ruime vriendenkring geweten dat zij hier aanwezig zijn. Ook uw gsm-signaal maakt duidelijk dat u hier bent.

Goede morgen,

1. Wij leven nu eenmaal in het tijdperk van de digitale revolutie, waarin ook de surveillancetechnologie zich met een adembenemende snelheid ontwikkelt. Ik wil het vandaag hebben over die nieuwe technologieën, maar ook over hoe die in samenspel met de tijdsgeest die door de gebeurtenissen van 9/11 gecreëerd werd en met de verregaande invloed van de Europese Unie op de besluitvorming, bepalen hoe uw privacy er vandaag uit ziet, of niet (goed) uit ziet.

2. Het is onbegonnen werk om de nieuwste controletechnologieën op vijf minuten samen te vatten. Elke dag verschijnt er wel een nieuwe doorbraak, een nieuw neusje van de zalm.

- Wat dacht u van de spionage drones (de onbemande vliegtuigjes) voor burgerlijke toepassingen, zoals BAE Systems, één van de grootste Europese wapenfabrikanten, nu ontwikkelt. Vanaf 2012 vliegen ze niet alleen meer in Afghanistan, maar ook boven uw hoofden als u manifesteert.*
- We dalen even terug af naar de aarde, naar de trams en bussen in Vlaanderen. 750 camera's installeerde vervoersmaatschappij De Lijn; in gewone bussen vier, in gelede bussen zes, in een tram acht. Met de cynische slogan 'Omdat we u zo graag zien'. 'Voor uw veiligheid is er camerabewaking in onze bussen en trams', luidt het, en dit terwijl er op 90% van de trams, sinds de afschaffing van de paardentram, nooit een noemenswaardig incident geweest is. Geen spijttechnologie, maar wel overdaadtechnologie. Nieuwe generaties camera's rukken op: met geluidssensoren om u niet alleen te zien maar ook te horen; met gezichtsherkenningsoftware die de boef uit een groep zou moeten halen; met intelligente software om abnormaal gedrag te detecteren; met nummerplaatregistraties voor het rekeningrijden.*

- *Maar camera's geraken stilaan achterhaald. Tegen 2013 zullen alle nieuwe auto's (verplicht of vrijwillig) uitgerust zijn met een 'communicatie box', waarmee de 'whereabouts' van chauffeurs waar ook in Europa kunnen getraceerd worden. Hieraan wordt volop gewerkt met CVIS (Cooperative Vehicle-Infrastructure Systems), een project van de EU waarin autobouwers en telecomindustrie samenwerken. De Europese Commissie heeft de regeringen al gevraagd om hiervoor een radiofrequentie te reserveren (op de 5.9 Gigahertz band). Het signaal van uw communicatie box kan opgepakt worden voor snelheidscontrole, rekeningrijden, het leiden van verkeersstromen... en zal voor gevolg hebben dat uw rijgedrag, maar ook waar u wanneer bent volledig wordt vastgelegd. Camera's zullen dan achterhaald zijn. Het nog met camera's werkende ANPR systeem in het Verenigd Koninkrijk registreert nu al dagelijks de nummerplaten van 10 miljoen auto's. Dit draconisch scenario hangt binnen enkele jaren alle Europese chauffeurs boven het hoofd. De impact hiervan op de privacy en op de persoonsgegevens is niet te overzien.*
- *Bovenaan staat de spitstechnologie om het telefoon- en internetverkeer te controleren. U weet dat de satellieten van Echelon, een door de VS opgezet spionagesysteem, in staat zijn om naar schatting 90% van het wereldwijde telefoon- en internetverkeer te onderscheppen en screenen. De drang om met machines alles op te slaan en te screenen is duizelingwekkend. Ik citeer het Pentagon: 'De datavolumes van de controle-opdrachten zullen tegen 2015 het niveau van yottabtes (10 bits tot de 24ste graad) bereiken'. Het gaat om een septillion bladzijden tekst. Een septillion is een ééntje met 24 nullen er achter. In de toekomst zullen gigantische datavolumes worden opgeslagen en doorploegd.*
- *In volle opmars zijn de chips met radio frequentie identificatie, de RFID-chips. Er zijn reeds miljarden chips in omloop voor allerlei toepassingen, van metroticket tot paspoort. Zo'n gechipt paspoort kan door je kleding, van op afstand, geactiveerd en gelezen worden via radio frequenties. Onlangs besloten het Brusselse MIVB, De Lijn, de Waalse Tec en de NMBS om de Mobip-pas met chipkaart tot de standaard te maken voor het Belgische openbaar vervoer. Chips en biometrie, en hun combinatie, zijn de nieuwste rages in de controletechnieken. Uw paspoortchip bevat weldra, verplicht, een RFID-chip met pasfoto en twee digitale vingerafdrukken. In de VS worden chips al ingeplant bij Alzheimerpatiënten. De lobby van de RFID verdedigt zonder gêne dat chips massaal bij mensen ingeplant worden. 'Dat zijn geen verre toekomstscenario's, maar staat al voor de komende jaren op stapel,' zegt die lobby.*
- *Ook in uw warenhuis wordt je koopgedrag nauwlettend geobserveerd. Warenhuisketen Colruyt kondigde enkele weken geleden aan zijn klanten op maat gesneden reclamefolders te zullen toezenden, zoals de betere kleermaker costuums en kledjes aanmeet aan uw slanke lijf. Op basis van uw klantenkaart zal uw geliefd grootwarenhuis promoten wat u moet kopen. Wij weten wat u eet, drinkt, wij kennen uw geliefd kuisproduct... Het individuele consumentenprofiel van zo'n miljoen klanten rolt uit de computers van Colruyt.*

Ik kan zo nog een tijdje doorgaan.

Naast de vele mogelijkheden die de moderne technologie biedt om het leven aangenamer, efficiënter of veiliger te maken, betekent deze ook een enorme uitdaging voor de privacy.

3. De politieke verantwoordelijken zouden erover moeten waken dat die nieuwe technologieën niet worden toegepast wanneer zij een bedreiging betekenen voor de privacy, maar, zeker na 9/11, gaat het ook hier de verkeerde kant op. Privacy is moeten wijken voor de veiligheidsobsessie.

Ik citeer prominenten die de balans opmaken van die post 9/11 evoluties.

J.F. Leclercq, procureur-generaal bij het Hof van Cassatie:

‘Bijna ging op 11 september 2001 de geest van het Europa van de Rechten van de Mens teloor.’

Jo Stevens, voorzitter van de Orde van Vlaamse Balies (nieuwjaarsspeech 2010):

‘Het gaat erom dat deze war on terror al jaren misbruikt wordt, onder het mom van bescherming van de burgers, om de bescherming van hun mensenrechten en rechten van verdediging te slopen.’

Thomas Hammarberg, de mensenrechtencommissaris van de Raad van Europa:

‘We moeten de persoonsgegevens beter beschermen om te vermijden dat Europa afglijdt naar de uitwassen van een bewakingsstaat.’

4. Een derde element dat de erosie van de grondrechten mee bevorderde is de besluitvorming door de Europese Unie. Op het terrein van politie en justitie werden de wetten – 80% van de wetgeving komt van ‘Europa’ – niet meer gemaakt door parlementen, maar door de Raad Justitie en Binnenlandse Zaken van de EU. Het was dus de uitvoerende macht die zich meester heeft gemaakt van de wetgevende macht. En deze miskennis van de trias politica is niet zonder averij gebleven voor de privacy. Ik denk hier aan het PNR-akkoord tussen de VS en de EU (lieft 18 gegevens van vliegtuigpassagiers worden overgemaakt) en aan de zeer betwiste dataretentierichtlijn. Nu het Europees Parlement ook iets te zeggen heeft op het terrein van politie en justitie komt er wat weerwerk, zoals we onlangs zagen met het afschieten van het SWIFT-akkoord.

Er is echter geen reden voor gerustheid. Het Stockholmprogramma dat de lijnen uittekent voor 2010-2014 duwt, ondanks de vele mooie woorden over de grondrechten, Europa verder in een richting waar veiligheid en controle de prioriteiten zijn.

5. Het cumulatief effect van de nieuwe technologieën en van de nieuwe bevoegdheden is verpletterend geweest voor de privacy. Het was alsof er een nieuwe noodtoestand werd afgekondigd. Er ontstond een echte toezichtstaat met een overheid die alles en iedereen controleert en registreert. Kafka en Orwell samen. Het resultaat is dat wij ons vandaag de vraag moeten stellen, ‘wat schiet er nog over van onze privacy’?.

Viviane Reding, de nieuwe EU-commissaris Justitie, zei onlangs dat de privacy van de Europeanen 'de grote uitdaging is voor het komende decennium'. Ik kan haar geen ongelijk geven. Het zal er in Europa het komende decennium vooral op aan komen om het niet bij mooie woorden over de mensenrechten te laten, maar in de praktijk de bescherming ervan te organiseren. De mooie woorden mogen niet haaks op de realiteit staan.

6. Zoals gezegd werd het gros van de privacybeperkende maatregelen ingevoerd in naam van 'uw veiligheid', in naam van de strijd tegen criminaliteit en terrorisme.

'In naam van uw veiligheid'. Veiligheid, strijd tegen het terrorisme, werd een codewoord – bijna een magisch woord – dat vele heilige huisjes zonder veel protest onderuit haalde.

Benjamin Franklin zei ooit dat 'wie vrijheid opgeeft in naam van de veiligheid, noch veiligheid noch vrijheid zal hebben.'

Het is dat wat, helaas, de voorbije jaren gebeurde. Vrijheid werd opgegeven in naam van de veiligheid.

Maar veiligheid is een slechte raadgever, veiligheid is een gevaarlijk concept om het beleid van de staat op te bouwen.

6.1. De terroristische aanslagen waren een objectieve basis voor een angstklimaat; iedereen reist wel met de metro en de trein, het terrorisme kon iedereen treffen. Dit klimaat heeft het mogelijk gemaakt dat grondrechten veel sneller ingeperkt werden, dan denkbaar zou zijn in normale tijden.

Het is evident dat de staten moeten reageren tegen het terroristisch gevaar, dat zij hun burgers tegen terreur moeten beveiligen. Maar er werd overgereageerd, de bescherming van de burgers werd als mom gebruikt. Aan de bevolking werd bovendien de illusie verkocht dat totale veiligheid mogelijk was.

Op mondiaal niveau stegen de uitgaven voor interne veiligheid sinds 2001 met zo'n 70 miljard dollar. Hier tegenover staat – en ik citeer uit de rede van procureur-generaal Leclercq – een gemiddelde van 420 slachtoffers per jaar wereldwijd. Vergeleken met de slachtoffers van honger, oorlogen, arbeidsongevallen, milieurampen, auto-ongevallen ... gaat het om een klein aantal. Ik wil hiermee de ernst van terroristische aanslagen niet minimaliseren, maar deze wel plaatsen in de juiste verhoudingen.

'We kunnen ons afvragen of de terroristen er niet in geslaagd zijn de ontwikkelde wereld veel verloren geld te doen investeren in het antiterrorisme, dit alles met verwaarlozing van dringende problemen zoals gezondheid, milieu, conflicten en bestuur.' Aldus Bjørn LOMBORG en Todd SANDLER (een Zweedse en een Amerikaanse prof), geciteerd door Leclercq.

Het veiligheidsbeleid heeft ervoor gezorgd dat op wereldvlak de noden en prioriteiten werden scheef getrokken.

6.2. Er werd in dat ganse veiligheidsbeleid ook verdedigd dat er een balans moest gevonden worden tussen veiligheid en vrijheid, tussen controle en privacy.

Een eerste vaststelling is dat die zogenaamde balans wel volledig is doorgeslagen in de richting van de veiligheid. De securitaire waan won het op de vrijheid.

Maar gaat die balanstheorie wel op? Is het – bekeken vanuit de mensenrechten – juist om vrijheid en veiligheid als twee gelijke waarden in de balans te leggen?

De Challenge Group, dit is een groep van professoren die, ter voorbereiding van het Stockholmprogramma, door de EU zelf in het leven werd geroepen om te adviseren over de verhouding tussen veiligheid en vrijheid zegt 'dat het fout is te geloven dat veiligheid en vrijheid twee analoge principes zijn en dat zij daarom kunnen vergeleken worden en tegen elkaar kunnen afgewogen worden. Vrijheid is een centrale waarde die terug te vinden is in de kern, niet alleen van de EU-verdragen, maar ook van alle internationale mensenrechtenverdragen'.

Ik deel die zienswijze. De balanstheorie trekt de verhouding tussen de vrijheden en de veiligheid volkomen scheef door beide op gelijke voet te plaatsen.

Natuurlijk moet de overheid ervoor zorgen dat de burgers veilig kunnen leven, maar dan met respect voor en op de grondslag van de vrijheden zoals de privacy die precies in leven werden geroepen (in reactie op het Ancien Régime) als een verweermiddel van de burger tegen te verregaand overheidsoptreden.

In plaats van een weegschaal-model moeten vrijheid (privacy) en veiligheid geplaatst worden in een pyramide. Met onderaan aan de basis van de pyramide de vrijheden van de burgers en daar bovenop de veiligheid. Het is zoals met een huis. Tegen de regen heb je een dak nodig, maar u kan op een huis geen dak zetten als je geen fundamenten hebt.

De overheid moet de veiligheid garanderen aan de burgers, maar dit kan enkel wanneer het hierbij de vrijheden als basis neemt.

Een andere reden waarom veiligheid niet in de balans met privacy kan gelegd worden is omdat het om een containerbegrip gaat, een breed begrip waar van alles kan in ondergebracht worden; veiligheid op het werk, in het openbaar vervoer, in de Brusselse volkswijken of op de luchthaven. Een afweging kan maar als het gaat om twee evenwaardige, maar ook om twee duidelijke en concrete rechten. Veiligheid beantwoordt niet aan dit criterium.

Privacy kan wel afgewogen worden (in de balans gelegd worden) met het recht op leven of het recht op fysieke integriteit. Dat zijn twee heel duidelijke en concrete rechten.

Hoe meer in een concrete situatie het leven van mensen bedreigd wordt, hoe meer het aanvaardbaar is dat inbreuk wordt gemaakt op de privacy. Hoe minder leven of fysieke integriteit in het gedrang komen, hoe minder afbreuk kan gedaan worden aan de privacy. Zo is concrete afweging wel mogelijk. Het is aanvaardbaar dat op de luchthaven van Zaventem (door bv fouillering, bodyscan...) strengere ingrepen tegen de privacy plaatsvinden, dan in een stad als Mechelen. Het leven van de mensen loopt in het algemeen grotere risico door een aanslag op een vliegtuig dan door een voorval op de grote markt van Mechelen. Dat er in Mechelen camera's worden opgehangen om criminaliteitsgevoelige plaatsen (bv het station, of een uitgangsbuurt) te controleren lijkt aanvaardbaar omdat daar door een vechtpartij of een diefstal de fysieke integriteit in het gedrang kan komen, maar dat de ganse stad Mechelen dan maar

meteen met camera's wordt uitgerust vindt geen enkele verantwoording bij de afweging tussen de privacy en het recht op fysieke integriteit van de Mechelaars.

6.3. Privacy is inderdaad geen absoluut recht. Artikel 8 van het EVRM laat toe om onder bepaalde voorwaarden inbreuken op de privacy van de burgers te plegen. Maar de regel is wel de bescherming van het privéleven, en de uitzondering is de inbreuk hier op. Ik zeg dit om dat de voorbije jaren een beleid werd gevoerd waarbij de uitzondering tot regel werd verheven. Overal camera's, in elk metroticket een RFID-chip, elke persoon die ergens met de politie in aanraking kwam in de ficher...

Uitzonderingen op de privacy moeten dan nog beantwoorden aan de gekende criteria van noodzaak en proportionaliteit. Zijn de inbreuken op de privacy echt noodzakelijk in een democratische maatschappij, en zo ja, zijn de genomen maatregelen niet buiten verhouding met het kwaad dat ze willen tegengaan?

Wanneer minister Crevits de invoering van de RFID-chip in de pasjes bij De Lijn verdedigt zegt ze dat dit nodig is 'om van het geleuter over de reizigersaantallen vanaf te zijn.' Dit heeft dus echt niets te maken met 'de noodzaak in een democratische maatschappij'.

Wanneer de Mechelse burgemeester zijn ganse stad volhangt met camera's omwille van de veiligheid en de criminaliteit is zulke maatregel totaal buiten proportie met het nagestreefde doel.

Jo Stevens: 'Advocaten ... hebben als eerste taak het recht ... tegen deze securitaire waan van de dag te beschermen'. Wanneer ik ben ingegaan over dit – mogelijk wat theoretische – debat over de balans, de pyramide en artikel 8 EVRM is het precies om 'het recht' te beschermen.

7. De tientallen controlemaatregelen die werden doorgevoerd hebben nog andere motieven dan de bescherming van de veiligheid, hoewel dit niet openlijk wordt verkondigd. Het veiligheidsdiscours dekt ook andere agenda's.

Ik som er enkele op.

7.1. Wanneer de trams en bussen boordevol camera's worden gehangen heeft dit ook te maken met de besparingen op het personeel. Naast de chauffeur op elke tram of bus en in de metrostellen – zoals dit in de jaren stilletens het geval was – een toezienend personeelslid plaatsen is waarschijnlijk veel effectiever voor de veiligheid dan die camera's, die trouwens preventief amper enig effect hebben.

7.2. De technologie-industrie is big business. Het is een groeiende sector. In de chipsindustrie wordt van 2008 tot 2018 een groei 4 miljard naar 20 miljard verwacht. De cameramarkt zal tot 2015 elk jaar met 45 procent groeien. De beveiligingsindustrie en de biometrie zijn bloeiende sectoren waarin grote technologiebedrijven en wapenfabrikanten nauw samenwerken. De EU heeft het budget voor het veiligheidsonderzoek opgetrokken naar 1,35 miljard.

De economie domineert de wereld. Deze simpele werkelijkheid wordt graag verstopt achter het gordijn van de noodzaak voor de veiligheid. Wanneer wij vaststellen dat het hoofd van

burgemeesters zo zot wordt gemaakt dat zij hun ganse stad vol camera's hangen dan wijst dit op succesvol lobbywerk en marketing van de industrie.

7.3. Stilaan geraakt de controle op de ganse bevolking georganiseerd. Alles en iedereen onder controle is de natte droom van elk autoritair regime. In het VK werd het hoogste spionagebudget ooit uitgetrokken voor een volledige screening van de islamgemeenschap. Ook daarvoor dienen de nieuwe technologieën. Naast de algemene controle geven ze de overheid ook de mogelijkheid om politieke en sociale bewegingen in de gaten te houden, vooral deze die niet in de mainstream lopen. Ik denk hier aan het voorval met de vier Luikse andersglobalisten. De nieuwe BLM-wet zal deze tendens nog versterken.

8. Ik wil besluiten met het volgende.

Er wordt gezegd dat 'de mensen niet wakker liggen van de privacy'. Er wordt door de baas van Facebook gezegd dat 'privacy een begrip is uit het verleden', want miljoenen burgers maken zonder bezwaar hun privéleven openbaar via zo'n sociaal netwerk. Er wordt door de Mechelse burgemeester, wanneer de Privacycommissie hem kritiseert omwille van zijn cameramanie, gezegd 'dat alleen boeven en gangsters hiervan schrik moeten hebben'.

Er wordt gezegd: 'Wie niets te vrezen heeft, heeft niets te verbergen.' Dit soort dooddoeners wordt verspreid en pakt ook nog verf.

En toch. De Eurobarometer 2008 gaf aan dat 64% van de EU-burgers 'tamelijk tot zeer ongerust' is over de bescherming van de persoonsgegevens.

Iedereen heeft inderdaad wel iets te verbergen. Niemand loopt graag te koop met zijn inkomen, gezondheid, vriendschappen ...

Het besef groeit dat er iets fundamenteels verkeerd aan het lopen is met de privacy. De burgers hebben zelf een verantwoordelijkheid om niet alle privégegevens zo maar te grabbel te gooien. Maar de kern van het probleem ligt niet daar. Het is goed dat de burgers maximaal gebruik maken van de enorme technologische mogelijkheden om bijvoorbeeld snel en wereldwijd met mekaar te communiceren. De hoofdverantwoordelijkheid voor de bescherming van de privacy ligt bij de overheid.

'Staten moeten verantwoorden wanneer zij zich inmengen in het privéleven, niet de individuele burger moet zich rechtvaardigen waarom hij zich bezorgd voelt over de inmenging in de grondrechten.' Dit zijn de woorden van Hammarberg.

Het is vanuit dit correcte uitgangspunt dat de bescherming van de privacy, 'de uitdaging voor het komende decennium', moet verdedigd worden.

De privacy is dood, leve de privacy.

Ik dank u.

SACRIFIER LE DROIT À LA VIE PRIVÉE AU NOM DE LA SÉCURITÉ? ANALYSE DE DÉVELOPPEMENTS RÉCENTS ET DE L'UTILISATION DE NOUVELLES TECHNOLOGIES.

Traduction

*Mesdames et Messieurs,
Chers Collègues,*

Vous avez déjà été filmés aujourd'hui par une dizaine de caméras. Certains d'entre vous ont été identifiés à distance quand ils ont utilisé pour venir ici leur carte MOBIB contenant une puce RFID (Identification par fréquence radio) dans le métro bruxellois. Les utilisateurs de Facebook parmi vous ont peut-être révélé à un large cercle d'amis qu'ils sont ici aujourd'hui. Le signal de votre GSM permet aussi de savoir que vous êtes présent ici.

Bonjour,

1. Nous vivons à l'époque de la révolution digitale au cours de laquelle la surveillance technologique se développe également à une vitesse époustouflante.

Je vous parlerai aujourd'hui des nouvelles technologies mais aussi de la façon dont celles-ci déterminent l'état de votre droit à la vie privée aujourd'hui (guère florissant) en combinaison avec le climat créé par les événements du 11 septembre 2001 et l'influence très significative de l'Union européenne a pris sur le processus de décisions.

2. Il est impossible en 5 minutes de donner un aperçu complet des nouvelles technologies de contrôle. Chaque jour une nouvelle percée en la matière apparaît.

- Que pensez-vous par exemple des drones (avions sans pilotes) d'espionnage pour des applications civiles, telles que BAE-systems, un des plus grand producteurs d'armes en Europe, les développe actuellement ? A partir de 2012, ils voleront plus souvent en Afghanistan, mais aussi au dessus de vos têtes quand vous manifesterez.*
- Redescendons sur terre, et plus spécialement, dans les trams et bus en Flandre. La société de transports De Lijn a installé 750 caméras: 4 dans les bus normaux, 6 dans les bus articulés et 8 dans les trams. A grand renfort de slogans cyniques tel que "parce que nous aimons tant vous voir" . « Pour votre sécurité il y a de la vidéosurveillance dans les bus et nos trams » nous dit-on. Et cela alors que sur 90 % des trams il n'y a jamais eu d'incidents significatifs depuis l'abolition du tram à cheval.
Il ne s'agit donc pas d'une technologie de pointe, mais d'une technologie superflue.*

- *De nouvelles générations de caméras sont maintenant installées: avec non seulement des capteurs de son, pour ne pas seulement vous voir, mais également pour vous entendre. Ces caméras peuvent être munies d'un logiciel de reconnaissance de visage qui devrait être capable d'isoler la brute dans le groupe, d'un logiciel « intelligent » pour détecter un comportement "anormal", et d'un logiciel de reconnaissance des plaques d'immatriculation pour une taxe routière en fonction de la distance parcourue.*
- *Notons que les caméras sont déjà en train de devenir des technologies démodées. En 2013, tous les nouveaux véhicules seront équipés (obligatoirement ou sur une base volontaire) d'une boîte de communication qui permet de tracer des véhicules n'importe où en Europe. Ce système est développé dans le cadre du CDIS (« Cooperative vehicle- infrastructure systems »), un projet de l'Union européenne auquel les constructeurs automobiles et l'industrie des télécommunications collaborent. La Commission européenne a déjà demandé aux gouvernements de réserver une radiofréquence pour ceci (sur la bande 5.9 gigahertz). Le signal de votre boîte de communications sera peut-être utilisé pour les contrôles de vitesse, pour une taxe perçue en fonction des kilomètres parcourus, pour la diriger les flux de circulation. Mais ceci aura surtout pour conséquence que vos déplacements et votre comportement sur la route seront entièrement enregistrés, où que vous soyez. Les caméras seront alors démodées. Le Royaume-uni utilise encore des caméras pour enregistrer quotidiennement les plaques d'immatriculation de 10 millions de véhicules. Un tel scénario draconien s'appliquera à tous les chauffeurs européens d'ici quelques années. L'impact sur la protection de la vie privée et des données personnelles est tout simplement impossible à mesurer.*
- *Les technologies de pointe pour contrôler les communications par téléphone ou par internet tiennent une bonne place dans notre inventaire. Vous savez que les satellites d'Echelon, un système d'espionnage monté par les USA, sont capables d'intercepter et de soumettre à un screening 90% des communications téléphoniques et par internet dans le monde. La volonté d'utiliser des machines pour enregistrer et de soumettre à un screening l'ensemble du trafic existe bel et bien. Je cite le Pentagone : "le volume des données à collecter dans le cadre des missions de contrôle aura atteint en 2015 le niveau yottabytes (10 bits au 24e degré). Il s'agit d'un équivalent d'un septillion de pages de texte. Un septillion est le chiffre 1 avec 24 zéros derrière. A l'avenir des volumes de données gigantesques seront enregistrées et soumises à analyse.*
- *La mode est aussi aux puces munies d'une identification par radiofréquence, les puces RFID. Il y a actuellement des milliards de ces puces en circulation pour toutes sortes d'applications, du ticket de métro jusqu'aux passeports. Un passeport contenant une telle puce peut être lu et activé à distance à travers les vêtements en utilisant des radiofréquences. Récemment la STIB, De Lijn, les TEC et la SNCB ont décidé d'utiliser la carte Mobib (contenant une puce RFID) comme standard pour les transports en commun en Belgique. Les puces et la biométrie et, surtout, la combinaison des 2, constituent une nouvelle tendance dans les techniques de contrôle. La puce dans le passeport contiendra bientôt la photo et 2 empreintes digitales. Aux Etats-unis les puces sont déjà implantées chez les patients qui souffrent de la maladie d'Alzheimer. Le lobby de la puce RFID défend sans gêne l'idée que les puces doivent être*

implantés massivement parmi la population. Il ne s'agit pas là d'un scénario de science-fiction, mais de plans concrets pour l'avenir, selon ce lobby.

- *Même au supermarché votre comportement de consommateur est observé de façon intense. La société Colruyt a annoncé il y a quelques semaines qu'on enverrait à ses clients des dépliants de publicité taillés sur mesure comme ceux du tailleur artisanal. Sur base de votre carte de client, votre supermarché préféré vous présentera ce que vous devez acheter. Nous savons ce que vous mangez, ce que vous buvez et quel est votre détergent préféré. Le profil de consommateur d'un million de clients sera donc contenu dans les ordinateurs de Colruyt.*

Je pourrais continuer comme ça encore longtemps.

Outre les énormes possibilités qu'offre la technologie moderne pour rendre la vie plus agréable, plus efficace ou plus sûre, elle comporte également un défi énorme pour la protection de la vie privée.

3. Les responsables politiques devraient veiller à ce que ces nouvelles technologies ne soient pas utilisées quand elles constituent une menace pour celle-ci. Mais depuis le 11 septembre 2001, l'évolution va certainement dans le mauvais sens. La protection de la vie privée a dû céder devant l'obsession de sécurité. Je voudrais citer quelques personnes influentes qui font le bilan des évolutions depuis le 11 septembre 2001.

J.F Leclercq, Procureur général à la Cour de cassation: "Le 11 septembre 2001 a bien failli faire perdre son âme à l'Europe des droits de l'homme."

Jo Stevens, Président de l'Ordre des Barreaux flamands dans son discours du nouvel an 2010: "Le problème est qu'on a abusé de la guerre contre le terrorisme depuis des années sous le prétexte de la protection des citoyens pour démolir la protection des droits de l'homme et des droits de la défense."

Thomas Hammarberg, le Commissaire aux droits de l'homme du Conseil de l'Europe: "Nous devons mieux protéger les données personnelles pour éviter que l'Europe glisse vers les excès d'un état de surveillance."

Un troisième élément qui a contribué à l'érosion des droits fondamentaux est le processus de prise de décisions dans l'Union européenne. Dans le domaine de la police et de la justice, les lois ne sont plus discutées par les parlements, mais proviennent à 80 % du Conseil des ministres de la justice et des affaires intérieures de l'Union européenne. Le pouvoir exécutif s'est donc rendu maître du pouvoir législatif. Cette méconnaissance de la séparation des pouvoirs n'est pas sans conséquences dommageables pour la protection de la vie privée. Je pense à l'accord PNR entre les États-unis et l'Union européenne (pas moins de 18 données concernant les passagers sont transmises) et à la très discutée directive sur la rétention des données. Depuis que le Parlement européen a son mot à dire sur le terrain de la police et de la justice, on observe une certaine résistance, comme nous l'avons vu récemment avec le rejet de l'accord Swift. Cela ne suffit néanmoins pas pour nous rassurer. Le programme de Stockholm qui trace les grandes lignes

pour la période 2010- 2014, malgré quelques belles phrases sur les droits fondamentaux, fixe à l'Europe une direction où la sécurité et le contrôle sont les principales priorités.

5. L'effet cumulatif des nouvelles technologies et des nouvelles compétences a eu l'effet d'un véritable rouleau compresseur pour la protection de la vie privée. Parfois, il semblerait qu'un nouvel état d'urgence a été décrété. Un état de contrôle dans lequel les autorités contrôlent et enregistrent tout et tout le monde. Il s'agit d'une inquiétante combinaison de Kafka et d'Orwell. Résultat ? Nous devons aujourd'hui nous poser la question suivante : que nous reste-t-il encore de notre vie privée ? Viviane Reding, le nouveau commissaire de l'Union européenne à la justice a déclaré récemment que la protection de la vie privée des Européens est "le grand défi pour la décennie à venir". Je ne peux pas lui donner tort. Dans les prochaines 10 années à venir, le problème de l'Europe sera surtout de ne pas s'en tenir à quelques belles paroles sur les droits de l'homme mais d'organiser dans la pratique leur protection. Les belles paroles ne peuvent pas être opposées à la réalité.

6. Comme je l'ai indiqué, la plupart des mesures qui portent atteinte à la vie privée ont été prises au nom de "votre sécurité", au nom de la lutte contre la criminalité et le terrorisme.

"Au nom de votre sécurité". La sécurité, la lutte contre le terrorisme, devient des codes, des mots magiques qui ont détruit sans beaucoup de protestations de nombreux droits qu'on croyait acquis pour l'éternité.

Benjamin Franklin a dit un jour que ceux qui abandonnent la liberté au nom de la sécurité n'auront ni sécurité, ni liberté. C'est hélas ce que nous avons pu constater les dernières années. La liberté a été sacrifiée au nom de la sécurité, mais la sécurité est mauvaise conseillère. Ce n'est qu'un concept dangereux qui ne peut servir comme fondement à une politique publique crédible dans ce domaine.

6.1. Les attentats terroristes constituent un fondement objectif pour justifier un climat d'angoisse: il arrive à tout le monde de prendre le métro ou le train. Le terrorisme peut donc nous toucher tous. Ce climat a rendu possible la limitation de droits fondamentaux à une vitesse fulgurante, ce qui était impensable en temps normal.

Il est évident que les états doivent réagir contre le danger terroriste et protéger leurs citoyens contre la terreur. Mais la réaction a été disproportionnée : la protection des citoyens a servi de prétexte. On a vendu à la population l'illusion qu'une sécurité totale était possible.

Depuis 2001, les dépenses de sécurité intérieure ont augmenté de près de 70 milliards de dollars au niveau mondial. « Les citoyens des pays riches considèrent le terrorisme international comme l'une des plus grandes menaces qui pèsent sur la planète, alors qu'il ne fait en moyenne que 420 victimes dans le monde chaque année » (je cite ceci du discours du Procureur général Leclercq). En comparaison avec le nombre de victimes de la faim, des guerres, des accidents de travail, des catastrophes écologiques, des accidents de la route... il s'agit d'un nombre peu élevé. Je ne veux pas ici minimaliser la gravité des attentats terroristes mais simplement les resituer à leurs justes proportions.

Selon Bjørn LOMBORG et Todd SANDLER (professeurs suisse et américain), cités par Leclercq, « on peut se demander si les terroristes n'ont pas réussi à faire que le monde développé investisse à fonds perdu dans le contre-terrorisme, tout en ignorant des problèmes urgents portant sur des questions de santé, d'environnement, de conflit ou de gouvernance? ».

La politique sécuritaire a donc forcé un traitement biaisé des besoins et des priorités au niveau mondial.

6.2. Dans le cadre de la politique de sécurité, on défend aussi l'idée que la sécurité doit être mise en balance avec la liberté, et que la surveillance devait être en équilibre par rapport à la vie privée.

Le premier constat, c'est que cette soi-disant balance penche complètement dans la direction de la sécurité. Le plateau sécuritaire pèse bien plus lourd que celui de la liberté.

Mais est-ce que cette théorie de la balance tient la route ? Est-il correct, d'un point de vue des droits humains, de mettre en balance la sécurité et la liberté comme deux valeurs égales ?

Le Challenge Group, un groupe de professeurs mis en place par l'UE pendant la préparation du programme de Stockholm pour donner un avis sur les relations entre liberté et sécurité a dit « il est faux de croire que la sécurité et la liberté sont deux principes analogues et qu'ils peuvent être comparés et mis en balance. La liberté est une valeur centrale qu'on retrouve dans le noyau dur, non seulement des traités de l'UE, mais aussi de tous les instruments des droits de l'homme au niveau international ».

Je partage cette façon de voir les choses. La théorie de la balance biaise totalement la relation entre sécurité et liberté en les mettant au même niveau. Les pouvoirs publics doivent bien évidemment veiller à ce que les citoyens puissent vivre en sécurité, mais ceci dans le respect des libertés fondamentales comme la vie privée, qui a précisément été mise en place (en réaction à l'Ancien régime), comme un moyen de défense du citoyen contre les abus de pouvoirs de l'autorité.

A la place du modèle de la balance, la liberté (vie privée) et la sécurité doivent prendre place dans une pyramide. En bas, à la base de la pyramide, figurent les libertés du citoyen, et, au dessus, la sécurité. Comme dans un bâtiment. Le toit est nécessaire pour protéger de la pluie, mais il est impossible de placer un toit en l'absence de fondations.

Les pouvoirs publics doivent garantir la sécurité aux citoyens, mais ceci n'est possible que si on considère les libertés comme un fondement préalable.

Une deuxième raison pour laquelle la sécurité ne peut pas être mise en balance avec la liberté, c'est qu'il s'agit d'un concept fourre-tout, d'une notion large dans laquelle on peut mettre tout et n'importe quoi : sécurité dans les transports, sur le lieu de travail, dans les quartiers populaires de Bruxelles ou dans l'aéroport. Une mise en balance n'est possible que lorsqu'on parle de choses équivalentes, mais aussi lorsqu'on parle de droits concrets et bien définis. La sécurité ne remplit pas ce critère.

La vie privée peut être mise en balance avec le droit à la vie ou le droit à l'intégrité physique. Il s'agit de deux droits très concrets. Plus le droit à la vie est menacé dans une situation concrète,

plus l'ingérence au droit la vie privée est acceptable. Moins la vie ou l'intégrité physique est en danger, moins il peut être porté atteinte à la vie privée. De cette façon, la mise en balance est bien possible. Des mesures attentatoires à la vie privée sont plus facilement acceptables dans l'aéroport de Zaventem (fouilles, bodyscan...) que dans une ville comme Malines. Le risque d'atteinte à la vie des personnes est, en général, plus important en cas d'attentat dans un avion que dans un incident sur la grand-place de Malines. Il peut sembler acceptable qu'on place à Malines des caméras de surveillance pour contrôler des lieux sensibles (la gare, un quartier de lieux de sorties) parce que l'intégrité physique peut y être mise en danger par un vol ou une bagarre. Mais que la ville de Malines soit du jour au lendemain équipée de caméras sur toute sa superficie ne trouve aucune justification dans la balance entre la vie privée et le droit à l'intégrité physique des Malinois.

6.3. La vie privée n'est pas un droit absolu. L'article 8 de la Convention européenne des droits de l'homme permet des ingérences dans la vie privée des citoyens à certaines conditions. Mais la règle reste le droit à la vie privée, et l'ingérence reste une exception. Il faut le rappeler parce que ces dernières années, la politique menée tend à ce que l'exception devienne la règle. Caméras partout, puce RFID dans chaque ticket de métro, fichage de toute personne qui entre en contact avec la police.

Les exceptions à la vie privée doivent aussi répondre aux critères traditionnels de nécessité et de proportionnalité. Les ingérences à la vie privée sont-elles nécessaires dans une société démocratique, et si oui, les mesures prises ne sont-elles pas disproportionnées en rapport avec le mal qu'elles prétendent combattre ?

Quand le ministre Crevits défend l'inclusion de puce RFID dans les titres de transport chez De Lijn, il dit que c'est nécessaire pour « en finir avec les discussions concernant le nombre de voyageurs ». Ceci n'a donc rien à voir avec une mesure « nécessaire dans une société démocratique ».

Lorsque le bourgmestre de Malines équipe toute la ville de caméras sous couvert de sécurité et de lutte contre la criminalité, une telle mesure est totalement hors de proportion avec le but poursuivi.

Jo Stevens: "La première tâche des avocats est de protéger le droit contre cette tendance sécuritaire". Quand j'ai abordé le débat – sans doute un peu théorique – sur la balance et la pyramide et l'article 8 de la CEDH, il s'agissait précisément de défendre « le droit ».

7. Les dizaines de mesures de surveillance qui sont appliquées ont encore bien d'autres motifs que la protection de la sécurité, bien que ceci ne soit pas ouvertement divulgué. Le discours sécuritaire cache aussi d'autres agendas.

Passons-en quelques un en revue.

7.1. Lorsque les trams et bus s'équipent de caméras, il s'agit aussi d'économies sur le personnel. Aux côtés du chauffeur dans chaque tram ou bus, ou stations de métro –c'était le cas encore il y a quelques années – on rencontrait un contrôleur qui était probablement beaucoup plus efficace que la vidéosurveillance, dont l'effet préventif semble pour le moins limité.

7.2. *L'industrie de la technologie est big business. C'est un secteur florissant. L'industrie des puces électroniques prévoit une croissance de 4 à 20 milliards entre 2008 et 2018. Le marché des caméras va grandir chaque année de 45 % d'ici 2015. L'industrie de la sécurité et de la biométrie en plein boom, repose sur la collaboration étroite entre de grosses firmes technologiques et les fabricants d'armes. L'UE a augmenté son budget pour la recherche en matière de sécurité à 1,35 milliard.*

L'économie domine le monde. Cette vérité simple est volontiers cachée par le prétexte de la nécessité de la sécurité. Lorsqu'on constate que des bourgmestres sont suffisamment inconscients pour équiper l'entièreté de leur ville de caméras, ceci résulte du lobby efficace du marketing de l'industrie.

7.3. *Petit à petit, la surveillance globale de la population s'organise. Le contrôle sur tout le monde est le rêve de tous les régimes autoritaires. Au Royaume-uni, on prévoit d'investir le plus gros budget d'espionnage jamais vu jusqu'ici pour procéder au « screening » de la communauté musulmane. Les nouvelles technologies sont aussi mises à contribution à cette fin. A côté du contrôle général, elles donnent aussi aux pouvoirs publics l'occasion de tenir à l'œil les mouvements sociaux et politiques, surtout ceux qui s'écartent de la pensée dominante. Je pense ici à l'incident impliquant quatre altermondialistes liégeois. La nouvelle loi sur les méthodes de recueil de données par les services de renseignement va encore renforcer cette tendance.*

8. *J'en viens à ma conclusion.*

On dit que « les gens ne se préoccupent plus de leur vie privée »

Le patron de Facebook prétend que "la vie privée est un concept du passé", parce que des millions de citoyens rendent public des éléments de leur vie privée à travers ce réseau social. Lorsqu'il est critiqué par la Commission pour la protection de la vie privée pour sa manie des caméras, le bourgmestre de Malines affirme que « seuls les délinquants et les gangsters doivent en avoir peur ». On entend souvent que « celui qui n'a rien à cacher n'a rien à craindre ». Ces sortes de slogans sont ressassés et largement diffusés. Et pourtant... Selon l'Eurobaromètre 2008, 64 % des citoyens de l'UE se montre « inquiet à très inquiet » au sujet de la protection des données personnelles. Tout le monde semble réellement avoir quelque chose à cacher. Personne ne souhaite que ses revenus, sa santé, ses amis... ne deviennent des données entièrement publiques. On prend peu à peu conscience qu'il y a quelque chose qui ne tourne pas rond actuellement avec la vie privée. Les citoyens ont eux-mêmes la responsabilité de ne pas répandre partout toutes leurs données personnelles. Mais le nœud du problème ne réside pas là. Il est bon que les citoyens fassent un usage maximal des énormes potentialités technologiques, par exemple pour communiquer rapidement entre eux dans le monde entier. La responsabilité principale pour la protection de la vie privée repose sur les épaules des pouvoirs publics. « Les Etats doivent se justifier lorsqu'ils s'immiscent dans la vie privée. Ce n'est pas au citoyen de s'expliquer pourquoi il se sent préoccupé par une atteinte à ses droits fondamentaux ». Ce sont les mots de Hammarberg.

C'est en partant de ce point de vue qu'il faut à présent défendre la protection de la vie privée comme « le défi de la décennie à venir ».

La vie privée est morte, vive la vie privée !

Je vous remercie.

POWERPOINT: PRIVACY OPGEVEN IN NAAM VAN DE VEILIGHEID

Privacy opgeven in naam van de veiligheid? Analyse van recente ontwikkelingen en het gebruik van nieuwe technologieën

Raf Jespers

Advocaat PROGRESS Lawyers Network
Colloquium Privacy 5 maart 2010



Schema

- I. Drie ontwikkelingen die de privacy vandaag beheersen
 - 1. *gebruik van nieuwe technologieën*
 - 2. *autoritaire klimaat na 9/11*
 - 3. *toegenomen invloed besluitvorming vanuit de Europese Unie (EU)*
- II. 'In naam van de veiligheid'. Realiteit en securitaire waan.
- III. Waar leidt dit toe? Controlemaatschappij.

I. 1. Gebruik van nieuwe technologieën

- Tijdperk van de digitale revolutie
- Surveillancetechnologie ontwikkelt zich met een adembenemende snelheid
- Totale controle – door overheid, economie... – wordt technisch mogelijk

Drone voor burgerlijke toepassing (BAE Systems)



Nieuwe technologie

- CAMERA'S
- Massaal gebruikt
- De Lijn op 750 bussen 'omdat wij u zo graag zien'
- Nieuwe generaties: geluidssensoren, gezichtsherkenning, registratie nummerplaten (rekening rijden), detectie abnormaal gedrag; intelligente software





Nieuwe technologie

- Auto communicatie box (CVIS-project)
- Satellieten, supercomputers voor screenen internet en telefoon; complexe algoritmeprogramma's
- Pentagon: 'Datavolumes van de controle-opdrachten zullen tegen 2015 het niveau van Yottabytes (10 bits tot de 24^{ste} graad) bereiken'; dit is een septillion bladzijden tekst (een eentje met 24 nullen er achter)
- RFID-chips (met biometrische gegevens)

Nieuwe technologie

- Datamining; inzameling en profilering; technisch eindeloze mogelijkheden; krankzinnig veel ingezameld
- Colruyt: via klantenkaart, consumptieprofielen van 1 miljoen klanten;
- Politiedatabank (1,6 miljoen); Europese databanken: interoperabiliteit;
- Dataretentierichtlijn EU: nooit eerder geziene uitholling recht op privacy (Vander Velpen)

I.2. 9/11

- Tijdsgeest: angst en controle; autoritair
- Hammarberg (2008): 'Persoonsgegevens beter beschermen om te vermijden dat europa afglijdt naar uitwassen bewakingsstaat'
- J.F. Leclercq (2009): 'Bijna ging op 11 september 2001 de geest van het Europa van de Rechten van de Mens teloor.'
- Jo Stevens (2010): 'Het gaat erom dat deze *war on terror* al jaren misbruikt wordt, onder het mom van bescherming van de burgers, om de bescherming van hun mensenrechten en rechten van verdediging te slopen'

'tijdsgeest': de bijzondere methoden

- BIM en BOM
- 'er wordt schaamteloos afgetapt' (De Hert); ook voor banale zaken; 4881 telefoons in 2008
- Politiek misbruik in zaak van andersglobalisten (arrest hof luik 3 december 2009)

I. 3. Europese Unie

- Besluitvorming justitie-politie door uitvoerende macht (Commissie, Raad)
- Diverse besluiten die privacy en andere grondrechten aantasten (twee kaderbesluiten terrorisme, dataretentierichtlijn, PNR-akkoord)
- Budget veiligheidsonderzoek; opgetrokken tot 1,35 miljard euro
- Stockholmprogramma (2010-2014): verder in de richting veiligheid en controle als prioriteit; wel besef probleem grondrechten



resultaat: 'Big brother'

- Samenloop van deze drie evoluties maakt dat privacy (en andere grondrechten) zwaar onder druk staan (zie swift-akkoord)
- Cumulatief effect van al die nieuwe technieken en bevoegdheden is verpletterend; alsof staat nieuwe noodtoestand afkondigt; de toezichtstaat; overheid controleert en registreert alles en iedereen. Kafka en Orwell samen
- Digitale revolutie is op zich geen slechte zaak; leven aangenamer, veiliger, democratischer; maar: geen almacht technologie ('alles wat technisch kan moet kunnen')
- Viviane Reding: privacy van de Europeanen is 'de grote uitdaging voor het komende decennium'

II. 'In naam van uw veiligheid'

- Veiligheidsdiscours (terrorisme, criminaliteit...) gebruikt en misbruikt
 - 'Autoritaire tijdsgeest; Securitaire waan van de dag' Jo Stevens (2010)
 - 1-scheeftrekken prioriteiten
 - 2-securitaire wint het op vrijheid; valse balanstheorie
 - 3-privacy geen absoluut recht (art. 8 EVRM)
-
-
-

II.1. scheefgetrokken prioriteiten

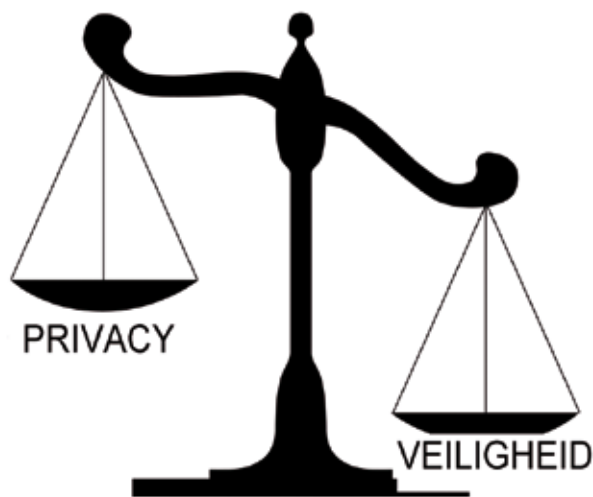
- Staat moet burgers tegen terreur beschermen
 - Stijging mondiale uitgaven sinds 2001 met 70 miljard dollar
 - 420 terreurslachtoffers per jaar
 - Lomborg en Sandler 'verloren geld'
-
-
-

II.2. Balans veiligheid – vrijheid?

- Balans doorgeslagen naar veiligheid
 - *Challenge Group: 'het is fout te geloven dat veiligheid en vrijheid twee analoge principes zijn en dat zij daarom kunnen vergeleken worden en tegen elkaar kunnen afgewogen worden; vrijheid is een centrale waarde die terug te vinden is in de kern, niet alleen van de EU-verdragen, maar ook van alle internationale mensenrechtenverdragen.'*
 - Veiligheid is containerbegrip, waarmee niet kan afgewogen worden.
-
-
-

II.2.bis Balans veiligheid – vrijheid?

- Wel balans privacy met recht op leven, recht op fysieke integriteit
- Pyramide in plaats van balans



II.3. Privacy geen absoluut recht

- Artikel 8 EVRM: principe privacy, uitzondering aantasting
- Uitzondering: legaliteit, noodzakelijkheid in democratische samenleving, proportionaliteit
- Afweging met grondrechten = basisbeginsel ipv afweging om redenen van economie of efficiëntie
- Camera's in alle bussen, in alle straten; RFID-chips in alle pasjes: niet noodzakelijk, buiten proportie

III. Waarom?

- Andere motieven dan 'veiligheid'
- -besparingen op personeel
- -big business: chipindustrie (4 miljard naar 20 miljard op tien jaar); cameramarkt: + 45% jaarlijks; EU-budget veiligheidsonderzoek: 1,35 miljard;
- -controle bevolking; toezicht op sociale en politieke bewegingen

Besluit

- Privacy is geen begrip uit het verleden; iedereen heeft iets te verbergen; 64% bekommerd
- Is afweerrecht van burger tegen staat en commercie; staten moeten inmenging verantwoorden, burgers moeten zich niet rechtvaardigen waarom zij bezorgd zijn
- Burger let best zelf ook wat op
- Geen verloren strijd (swift...)
- 'De privacy is dood, leve de privacy'

Beknopte biografie

Raf Jaspers behaalde zijn diploma van licentiaat geschiedenis aan de universiteit van Gent in 1972 en zijn diploma van licentiaat in de rechten in 1974.

Hij is al meer dan 30 jaar actief in het strafrecht, administratief recht, vreemdelingenrecht en vzw's.

Raf Jaspers is secretaris-generaal van de International Association of People's Lawyers (I.A.P.L.) en lid van de Liga voor Mensenrechten.

Hij heeft verscheidene publicaties op zijn naam staan, zoals 'De uitbouw van de Europese repressie'. Samen met Edith Flamand is hij co-auteur van 'Je rechten bij openbare actie'. Raf Jaspers is vaak gastspreker op seminars in binnen- en buitenland. In juni 2005 leverde hij een actieve bijdrage aan het congres van de International Association of Democratic Lawyers in Parijs en in oktober 2006 woonde hij het congres van de International Association of People's Lawyers bij in Davao, Filippijnen.

In het voorjaar 2010 verschijnt zijn nieuwste publicatie "Big Brother in Europa". In dit boek zet Raf Jaspers alles op een rij. Het resultaat is hoogst explosief.

Raf Jaspers a obtenu sa licence en Histoire à l'Université de Gand en 1972 avant d'obtenir sa licence en Droit en 1974.

Il est actif depuis déjà 30 ans en droit pénal, droit administratif, droit des étrangers et des associations.

Il est secrétaire-général de l'IAPL (International Association of People's Lawyers) et est membre de la Ligue flamande des Droits de l'Homme. Il a plusieurs publications à son compte : « Je rechten bij openbare actie » et « la construction de l'Europe de la répression ». Raf Jaspers intervient souvent comme orateur dans différents congrès et séminaires. Il poursuit son engagement au niveau international. Ainsi, il participa activement au Congrès de l'Association Internationale des Juristes Démocrates qui s'est tenu en juin 2005 à Paris et contribua au Congrès de l'IAPL à Davao aux Philippines. Sa dernière publication "Big Brother in Europa" paraît au printemps 2010. Raf Jaspers fait le point et le résultat est explosif.

1. Inleiding

In het eerste deel van dit hoofdstuk worden de algemene principes van privacybescherming in de arbeidssfeer uiteengezet. De verhouding tussen het grondrecht op privacy van de werknemer en het recht op toezicht van de werkgever wordt nader bekeken, samen met de vereisten waaraan alle regelgeving op dit gebied moet voldoen.

Het tweede deel gaat in op de manier waarop dit evenwicht in de Belgische regelgeving wordt vervat in de verschillende fasen van een arbeidsrelatie: de aanwerving, uitvoering en de beëindiging van een overeenkomst.

2. Algemene beginselen

Arbeid, ondergeschiktheid en toezicht

“De arbeidsovereenkomst voor werklieden is de overeenkomst waarbij een werknemer, de werkman, zich verbindt, tegen loon, onder gezag van een werkgever in hoofdzaak handarbeid te verrichten. De arbeidsovereenkomst voor bedienden is de overeenkomst waarbij een werknemer, de bediende, zich verbindt, tegen loon, onder gezag van een werkgever in hoofdzaak hoofdarbeid te verrichten.” In deze enigszins archaïsche bewoording beschrijft de Arbeidsovereenkomstenwet¹ de verhouding tussen werkgevers en werknemers. Abstractie makend van het steeds verder vervagende onderscheid tussen bedienden en arbeiders is er één karakteristiek die in het bijzonder relevant is voor de doeleinden van dit hoofdstuk: het gezag van de werkgever.

De arbeidsverhouding is per definitie een gezagsverhouding waarbij een bepaalde ondergeschiktheid wordt georganiseerd en in stand gehouden, met instemming van de betrokken partijen. Het gaat om een juridische ondergeschiktheid, die eruit bestaat dat de werkgever het recht krijgt om zijn werknemers instructies te bezorgen over de uitvoering van hun taken², en om de naleving van deze instructies te controleren. Dit impliceert noodzakelijkerwijze dat de werkgever in elke fase van de arbeidsrelatie een bepaald en beperkt indringingsrecht heeft in de persoonlijke levenssfeer van zijn personeel. De vraag stelt zich daarbij hoe ver een dergelijke inbreuk mag gaan.

¹ Meerbepaald artikelen 2 en 3 van de Wet van 3 juli 1978 betreffende de arbeidsovereenkomsten, B.S. 22 augustus 1978.

² Zie onder meer artikel 17 van de Arbeidsovereenkomstenwet, in het bijzonder lid 1 en 2: “Artikel 17. De werknemer is verplicht :

1° zijn werk zorgvuldig, eerlijk en nauwkeurig te verrichten, op tijd, plaats en wijze zoals is overeengekomen;

2° te handelen volgens de bevelen en de instructies die hem worden gegeven door de werkgever, zijn lasthebbers of zijn aangestelden met het oog op de uitvoering van de overeenkomst;”

Evenwicht tussen privacy en controlerecht

Zoals ook in andere hoofdstukken wordt beklemtoond is privacy een grondrecht waarvan de uitwerking en uitoefening aan beperkingen is onderworpen. In deze afdeling bekijken we nader onder welke voorwaarden er een inbreuk mag worden gemaakt op dit grondrecht.

Principes

Zoals hierboven al werd aangehaald heeft het grondrecht op privacy een aantal juridische weerslagen, waaronder artikel 8 van het Europees Verdrag van de Rechten van de Mens:

Artikel 8 - Recht op eerbiediging van privéleven, familie- en gezinsleven

- 1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
- 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.*

Waar de eerste paragraaf de principiële bescherming van de persoonlijke levenssfeer voorschrijft (inclusief het familieleven, woning en briefgeheim) bevat de tweede paragraaf de mogelijkheid om hierop uitzonderingen te maken. Het statuut van grondrecht impliceert immers geenszins dat beperkingen op de uitoefening ervan niet toegelaten zouden zijn. Daarentegen heeft dit wel tot gevolg dat men nooit volledig afstand doet van zijn persoonlijke levenssfeer door in een nieuwe relationele sfeer te treden. Dit geldt ook voor arbeidsrelaties, waar het recht op privacy weliswaar wordt ingeperkt, maar nooit volledig kan worden uitgesloten, zelfs niet met de uitdrukkelijke toestemming van de werknemer.

Het criterium voor de beoordeling van de toelaatbaarheid van deze uitzonderingen is de noodzakelijkheid ervan in een democratische samenleving. Dit criterium is in feite driedig: de beperkende maatregel moet worden gekenmerkt door legaliteit (d.w.z. de inmenging werd voorzien bij wet in de brede zin van het woord, m.a.w. een rechtsnorm), legitimiteit (d.w.z. de inmenging bestaat ter vrijwaring van één van de limitatief opgesomde waarden) en proportionaliteit (d.w.z. de inmenging is slechts toegelaten voor zover nodig in een democratische rechtsstaat)³. Artikel 8 heeft rechtstreekse werking in de Belgische rechtsorde voor zover het artikel inmenging in het privé- en familieleven van een individu verbiedt. Men kan er zich dus rechtstreeks op beroepen in een geschil.

³ Voor een meer uitgebreide bespreking verwijzen we naar het Hoofdstuk I: Algemene inleiding

Het is duidelijk dat toezicht door de werkgever niet per definitie strijdig is met artikel 8. De uitoefening van zijn gezag is immers nodig voor de bescherming van zijn rechten en vrijheden, en is in het belang van het economisch welzijn van zijn onderneming in haar geheel. De legitimiteit van elke maatregel zal verder moeten worden onderzocht, waarbij onder meer de finaliteit een centrale rol speelt. Verder zullen de maatregelen die de werkgever neemt eveneens moeten voldoen aan de andere voorwaarden van artikel 8, met name legaliteit en proportionaliteit. Het gaat om open criteria, waarvan de draagwijdte steeds in concreto zal moeten worden geapprecieerd in geval van betwistingen.

Een werknemer stelt zich vrijwillig (of minstens consensueel) onder het gezag van een werkgever, en aanvaardt daardoor impliciet een beperking op zijn privacy. De vermenging tussen zijn persoonlijke levenssfeer en zijn arbeidssfeer legitimeert als het ware het bestaan van een inperking. De vraag is dan vooral hoe ver deze beperkingen mogen gaan, in welke mate zij aan de voorafgaande toestemming van de werknemer zijn onderworpen, en aan welke voorwaarden zij moeten voldoen. Deze vraag wordt in de afdelingen hieronder nader bekeken.

Een bijzondere hypothese doet zich voor bij de zogenaamde “tendensondernemingen”, waarbij één of meerdere hoofdoogmerken van de onderneming in het teken van een bepaalde ideologie of overtuiging staat⁴. Men kan dan met name denken aan ondernemingen en instellingen die een bepaalde politieke, godsdienstige of charitatieve doelstelling hebben. Vermits het finaliteitsbeginsel impliceert dat de omvang van een inbreuk mede verantwoord kan worden door de specifieke aard van de onderneming, zou men kunnen argumenteren dat een verdergaande privacy-inbreuk bij werkgevers van deze bedrijven verantwoord is. Hieronder zal worden nagegaan in welke mate deze redenering opgaat.

Werknemers en zelfstandigen

De aandachtige lezer zal reeds gemerkt hebben dat de uiteenzetting hierboven in hoofdzaak is toegespitst op arbeidsrelaties, inzonderheid de contractuele verhouding tussen werkgevers en hun werknemers, eerder dan professionele relaties in het algemeen. Dit is geen toeval: het is namelijk enkel de arbeidsverhouding die door een band van ondergeschiktheid wordt gekenmerkt⁵. Wanneer men een beroep doet op zelfstandigen ontbreekt deze juridische ondergeschiktheid (wat in de praktijk economische ondergeschiktheid natuurlijk niet uitsluit), waardoor de vraag naar de toelaatbaarheid van een inbreuk op de privacy van een zelfstandige zich veel minder prangend stelt.

Immers, de zelfstandige wordt geacht op juridisch gelijke voet te staan met zijn opdrachtgever, waardoor hij in staat moet zijn om zijn persoonlijke levenssfeer zelf beter te handhaven. Hoewel dit in de praktijk zeker niet impliceert dat hij steeds over voldoende feitelijke autonomie beschikt om zijn belangen op de gewenste manier te behartigen zal in de uiteenzetting hieronder blijken dat de wetgever zijn bescherming voor een groot deel beperkt heeft tot werknemers. Het statuut en de rechten van de zelfstandige worden hieronder

⁴ F.HENDRICKX, “Privacy en arbeidsrecht”, Jura Falconis, 1998-99, 4, p.5.

⁵ We maken hier vanzelfsprekend abstractie van het fenomeen van de schijnzelfstandigheid. Hoewel deze verschijningsvorm van een arbeidsrelatie een reeks eigen problemen met zich meebrengt die eigen zijn aan zijn dubieuze statuut (en dit in elke relevante rechtstak), overstijgt een uitgebreide analyse van de gevolgen voor de persoonlijke levenssfeer de grenzen van deze uiteenzetting. We merken desondanks op dat er een opmerkelijke tendens groeit om niet enkel de aanwezigheid van gezag als criterium van onderscheid tussen zelfstandigen en werknemers te beschouwen, maar ook het bestaan van een economische afhankelijkheid. Dat dit het probleem allerminst eenduidig oplost is evident.

dan ook enkel besproken in zoverre dit relevant is (wat bijvoorbeeld en met name het geval zal zijn voor de toepassing van de Privacywet).

3. Arbeidsorganisatie en systematisch toezicht

Het aangaan van een arbeidsrelatie: kandidatenprospectie en sollicitaties

Eén van de belangrijkste momenten binnen de arbeidsrelatie is de aanvang ervan. Om de geschiktheid van een bepaalde kandidaat voor een bepaalde positie te kunnen inschatten is het van belang dat de potentiële werkgever kan peilen naar welk vlees hij in de kuip heeft. Het doel van de sollicitatieprocedure is dan ook de doelgerichte uitwisseling van relevante informatie.

Voor de informatiestroom van sollicitant naar potentiële werkgever impliceert dit dat deze laatste zoveel mogelijk betrouwbare informatie wil verzamelen over de kandidaat, terwijl de kandidaat er een belang bij heeft zichzelf zo goed mogelijk voor te stellen. Dit kan in sommige omstandigheden impliceren dat hij bepaalde informatie liever onderbelicht, verzwijgt, of dat hij zelfs vlakaf liegt. Voor de doeleinden van dit hoofdstuk is de centrale vraag op welke informatie de werkgever recht heeft, en hoe de sollicitant zich mag of moet gedragen.

In het licht van de hierboven gemaakte opmerkingen over de draagwijdte van artikel 8 van het EVRM en het recht op privacy in het algemeen zal duidelijk zijn dat de nood aan informatie van de werkgever slechts een beperkte indringing in de persoonlijke levenssfeer van de kandidaat kan verantwoorden. Zonder op de details vooruit te lopen kan nu al worden gesteld dat aan de eisen van proportionaliteit, legaliteit en legitimiteit moet worden voldaan. Grotendeels kunnen deze eisen worden veralgemeend naar de regel dat inbreuken in de persoonlijke levenssfeer van een sollicitant slechts toelaatbaar zijn indien de aard van het werk de inbreuk verantwoordt. Hieronder bekijken we wat dit in de praktijk inhoudt.

Werving en selectie

De belangrijkste Belgische rechtsnorm op het gebied van privacybescherming tijdens het sollicitatiegesprek is CAO nr. 38 van 6 december 1983 betreffende de werving en selectie van werknemers. Deze CAO is gedeeltelijk (artikel 1 t/m 6 en artikel 19) algemeen verbindend verklaard via het KB van 11 juli 1984⁶, en werd sinds zijn inwerkingtreding meermaals herzien. Dit impliceert dat enkel de eerste helft van de CAO juridisch bindend is, terwijl het tweede deel slechts aanbevelingen bevat. Niettemin kan een overtreding van de aanbevelingen als een indicatie worden beschouwd van het bestaan van een onrechtmatige daad in hoofde van de werkgever, zodat ook hieraan juridische gevolgen verbonden zijn.

⁶ Collectieve arbeidsovereenkomst nr. 38 van 6 december 1983 betreffende de werving en selectie van werknemers, gewijzigd door de collectieve arbeidsovereenkomsten nr. 38 bis van 29 oktober 1991, 38 ter van 17 juli 1998, nr. 38 quater van 14 juli 1999 en nr. 38 quinquies van 21 december 2004, algemeen verbindend verklaard door het KB van 11 juni 1984 (artikelen 1 tot 6), B.S. 28 juli 1984.

Hieronder gaan we even in op de rechten en de plichten van de betrokken partijen. Er zal blijken dat de normen van CAO 38 meestal vrij breed worden geformuleerd, en dat zij steeds in concreto moeten worden geapprecieerd. Dit is een kenmerk dat inherent is aan de spanning tussen de legitieme belangen van beide partijen, waarbij geen van beiden noodzakelijk als prioritair kan worden aangemerkt.

1) Plichten van de potentiële werkgever

De CAO huldigt twee grote principes bij de bepaling van de plichten van de werkgever: enerzijds non-discriminatie, anderzijds legitimiteit.

Voor het principe van non-discriminatie is artikel 2bis van de CAO de voornaamste grondslag. Het artikel verplicht de aanwervende werkgever om de sollicitanten tijdens de procedure gelijk te behandelen. Daarbij mag hij geen onderscheid maken op grond van persoonlijke elementen, wanneer deze geen verband houden met de functie of met de aard van de onderneming, behalve indien dit wettelijk wordt vereist of toegelaten. Informatie die louter tot de persoonlijke levenssfeer behoort mag dus in principe geen criterium vormen om de geschiktheid van een persoon voor een bepaalde functie te beoordelen.

Bij wijze van voorbeeld bevat het artikel ook een lijst van elementen die in het bijzonder niet als criterium mogen worden gehanteerd. Het gaat om leeftijd, geslacht, burgerlijke stand, ziekteverleden, ras, huidskleur, afkomst of nationale of etnische afstamming, politieke of levensovertuiging en lidmaatschap van een vakbond of een andere organisatie, seksuele geaardheid, of handicap van de sollicitant.

Nochtans is deze regel niet absoluut, en moet de toepassing ervan getemperd worden door een legitimiteitsafweging. In bepaalde gevallen kan een functie bijzondere eisen stellen aan de geschiktheid van een persoon die de werkgever enkel kan beoordelen door in diens persoonlijke levenssfeer binnen te dringen. Bij wijze van voorbeeld kan verwezen worden naar een sollicitatie voor een betrekking als laborant in een bloedinzamelingskliniek waar HIV-patiënten uit de sollicitaties worden geweerd.

Een controversiëler voorbeeld betreft de hierboven vermelde tendensondernemingen, die een bepaalde ideologie of overtuiging proberen uit te dragen. Men kan op een verdedigbare manier argumenteren dat deze ondernemingen er een legitiem belang bij hebben om kandidaten te weigeren wiens persoonlijke levensstijl op een bijzondere manier botst met de filosofie van de gewenste werkgever. Hierbij zal er echter dezelfde belangenafweging moeten worden gemaakt, waarbij er in het bijzonder zal worden gelet op de invloed die de persoonlijke levensstijl van een kandidaat al dan niet heeft op zijn geschiktheid voor een bepaalde functie.

Zo zal bijvoorbeeld een sollicitant die publiekelijk een bepaald godsdienstig radicalisme nastreeft daardoor sneller geweigerd kunnen worden voor een functie die religieuze neutraliteit vereist dan iemand die zijn geloof zelfs in een fanatieke variant enkel in familiale kring belijdt. Het aanhoudende publieke debat over de toelaatbaarheid van religieuze symbolen bij beoefenaars van een openbare functie toont echter al aan dat dit zelden een eenvoudige afweging is.

Teneinde de sollicitanten toe te laten om hun geschiktheid voor een functie zelf te beoordelen schrijft het (niet algemeen verbindende) artikel 8 de werkgever overigens voor dat hij in zijn werkaanbieding reeds

bepaalde informatie moet verstrekken. Het gaat onder meer over de aard van de functie en de eisen om de functie uit te oefenen.

Het hierboven beschreven artikel 2bis heeft echter enkel betrekking op de behandeling van de sollicitanten tijdens de procedure. Het artikel schrijft dus niet voor welke vragen een werkgever al dan niet mag stellen. Deze problematiek wordt geregeld door artikel 11. Hoewel dit artikel niet algemeen verbindend werd verklaard kan de overtreding ervan desondanks een onrechtmatige daad opleveren waarvoor de werkgever krachtens artikel 1382 B.W. tot een schadevergoeding kan worden veroordeeld. Dit vereist dan wel dat de gekrenkte kandidaat het bestaan en de omvang van een bepaalde schade kan aantonen, wat veelal geen sinecure is.

Artikel 11 verplicht de werkgever om de persoonlijke levenssfeer van de sollicitant bij de selectieprocedure te eerbiedigen, en "(z)ulks impliceert dat vragen over het privéleven slechts verantwoord zijn indien zij relevant zijn wegens de aard en de uitoefeningsvoorwaarden van de functie." Dit principe werd overigens al voor de totstandkoming van CAO 38 erkend⁷. Hier wordt met andere woorden een beroep gedaan op het legitimiteitscriterium: een vraag die de persoonlijke levenssfeer van de sollicitant schendt mag enkel worden gesteld indien de bijzondere aard en de voorwaarden van de functie dit verantwoorden. In feite is dit een andere benadering van het hierboven vermelde probleem: artikel 2bis verbiedt discriminatie op basis van irrelevante criteria; artikel 11 verbiedt zelfs dat hierover vragen worden gesteld.

Een typevoorbeeld is de vraag naar een eventuele relatie of kinderwens waarmee met name jongere vrouwelijke sollicitantes vaak worden geconfronteerd. De vraag houdt evident slechts zeer uitzonderlijk verband met de uitoefening van een functie, en is meestal enkel bestemd om de werkgever toe te laten om de kans op zwangerschapsverlof in te schatten. Behoudens zeer uitzonderlijke omstandigheden (zoals werk dat een bijzondere dreiging impliceert voor zwangere vrouwen, bijvoorbeeld door frequent contact met potentieel risicovolle chemicaliën) zal deze vraag strijdig zijn met artikel 11, en een sollicitante die kan aantonen dat ze ermee werd geconfronteerd zal dan ook aanspraak kunnen maken op een schadevergoeding.

Desondanks zet deze bepaling in de praktijk weinig zoden aan de dijk. Op de eerste plaats is er immers het bewijsprobleem: werkgevers zullen meestal geneigd zijn om potentieel inbreukmakende vragen enkel mondeling te stellen, en achteraf weigeren te bevestigen dat de kwestie op tafel werd gelegd. Daarnaast is er nog het probleem dat een schadevergoeding voor de sollicitant slechts vijgen na Pasen is. Op het moment dat een dergelijke irrelevante en inbreukmakende vraag wordt gesteld heeft de sollicitant immers veelal slechts twee reële keuzes: enerzijds de ongunstige waarheid vertellen of weigeren te antwoorden (waaruit de werkgever telkens dezelfde ongunstige conclusie zal trekken), of anderzijds liegen. Mag de sollicitant liegen om zijn persoonlijke levenssfeer te beschermen?

Dit is een controversiële vraag waarop het antwoord niet eenduidig vaststaat. Minstens moet worden beklemtoond dat de sollicitant ook een plicht heeft tot loyale informatieverstrekking, en dat hij waarachtig

⁷ Zie voor een vroege toepassing Arbrb. Gent 18 mei 1981, R.W. 1981-1982, 1426; J.T.T. 1981, 300.

dient te antwoorden op de vragen van de werkgever die relevant zijn voor de betrokken functie. Maar dit antwoord is onbevredigend: enerzijds geeft het geen uitsluitel over het bestaan van een “liegrecht” bij irrelevante vragen, en anderzijds leidt het in de praktijk ertoe dat de sollicitant de rechter wordt in de beoordeling van de relevantie.

Het antwoord op de vraag wordt veelal gezocht in een teleologische interpretatie van de relevantiebeperking. Indien de werkgever vragen stelt die een inbreuk maken op de persoonlijke levenssfeer van de sollicitant en die niet relevant zijn rekening houdend met de beoogde functie, dan verliest hij hierdoor impliciet zijn “recht op waarheid” dat zich immers enkel uitstrekt tot relevante informatie. In deze situatie is er dus inderdaad sprake van een liegrecht. Om het hierboven vermelde probleem van de “rechter in eigen zaak” te vermijden voegt de rechtsleer hier vaak aan toe dat het liegrecht een schild is, geen zwaard. Het mag met andere woorden enkel worden gebruikt om ongeoorloofde inbreuken op de persoonlijke levenssfeer af te slaan, en enkel wanneer andere middelen hiervoor niet zouden volstaan⁸.

Ten slotte verduidelijken artikel 11 en 12 van CAO 38 dat de verplichting om de privacy van de sollicitant te respecteren niet beperkt is tot de werkgever tijdens de sollicitatieprocedure. Ook andere personen die aan de selectiewerkzaamheden deelnemen (zoals bedrijfspsychologen en –geneesheren) dienen onnodige inbreuken te vermijden. Dit impliceert ook dat alle inlichtingen betreffende de sollicitant vertrouwelijk moeten worden behandeld door alle betrokkenen, en dit ook na de (al dan niet succesvolle) sollicitatie⁹.

2) Plichten van de aspirant-werknemer

Ook de plichten van de sollicitant komen aan bod in de CAO. Zijn belangrijkste plicht is de medewerking te goeder trouw aan de selectieprocedure (artikel 13). Dit impliceert dat hij alle noodzakelijke gegevens over zijn beroeps- en studieverleden moet verschaffen wanneer deze relevant zijn voor de geambieerde functie. Zoals hierboven al werd aangehaald is de verplichting zelfs nog iets ruimer dan in de CAO wordt vastgelegd: ook vragen die binnendringen in de persoonlijke levenssfeer moeten waarachtig worden beantwoord, indien zij aan het relevantiecriterium voldoen.

Een hieraan verbonden vraag is het al dan niet bestaan van een “spreekplicht” met betrekking tot persoonlijke informatie in hoofde van de sollicitant. In feite gaat het om het spiegelbeeld van het hierboven besproken “liegrecht”: als de sollicitant het recht kan hebben om onwaarachtig te antwoorden op irrelevante vragen, heeft hij dan ook de verplichting om op eigen initiatief relevante (en bij redelijke veronderstelling ongunstige) persoonlijke informatie te verstrekken die de werkgever verzuimt te vragen?

Deze vraag wordt overwegend positief beantwoord: de sollicitant dient uit eigen beweging alle nodige informatie te verstrekken waarvan hij weet dat deze relevant is voor en een substantiële invloed heeft op de beslissing van de werkgever¹⁰. Dit impliceert niet dat de werkgever zelf geen enkele onderzoeksplicht

⁸ F.HENDRICKX, “Privacy en arbeidsrecht”, Jura Falconis, 1998-99, 4, p.7.

⁹ Een schending van deze vertrouwelijkheidsplicht zou overigens strafbaar kunnen zijn, bijvoorbeeld als een schending van de Privacywet (cf.infra).

¹⁰ B.OVERSTEYNS, “Recht op informatie van werkgever, recht op privacy van de sollicitant. Enkele juridische problemen rond sollicitatie en aanwerving”, Or. 1988, 178 en volgende.

draagt. Wanneer de werkgever kennis heeft of zou moeten hebben van bepaalde informatie, dan is de sollicitant niet verplicht om opnieuw hierop te wijzen. De sollicitant kan immers niet verantwoordelijk worden gehouden voor de onachtzaamheid van de werkgever.

Dit is overigens niet meer dan logisch volgens het algemeen verbintenissenrecht. In elke overeenkomst zijn de partijen immers gehouden hun tegenpartij de informatie te bezorgen waarvan zij weten of behoren te weten dat deze een doorslaggevende invloed zou kunnen hebben op de instemming van de tegenpartij.

Net als de werkgever is ook de sollicitant nog na de sollicitatieprocedure gehouden tot een bepaalde vertrouwelijkheidsplicht. Artikel 14 van de CAO verbiedt hem om ruchtbaarheid te geven aan eventuele vertrouwelijke gegevens waarvan hij kennis zou hebben gekregen naar aanleiding van de sollicitatieprocedure.

Medische onderzoeken

Mede onder Amerikaanse invloed vindt ook in Belgische ondernemingen steeds vaker de gewoonte ingang om kandidaten niet alleen aan een ondervraging maar ook aan een medisch onderzoek te onderwerpen. Hoewel deze maatregel in beperkte mate en voor bepaalde posities zeker zinvol is, spreekt het voor zich dat hierbij de nodige terughoudendheid moet worden uitgeoefend omwille van de soms ernstige inbreuk op de persoonlijke levenssfeer die dergelijke onderzoeken vormen. Daarbij heeft de sollicitant minder mogelijkheden om zichzelf af te schermen tegen ongeoorloofde privacyinbreuken: de uitoefening van een "liegrecht" is immers weinig evident in een medisch onderzoek.

Eén van de bepalende criteria om de legitimiteit van een medisch onderzoek in het kader van een sollicitatiegesprek te beoordelen is het al dan niet wettelijk verplichte karakter ervan. We bekijken hieronder zowel de hypothese van een wettelijk verplicht onderzoek als van een onderzoek op vrij initiatief van de toekomstige werkgever.

1) Wettelijk verplicht medisch onderzoek

De Codex over het welzijn op het werk is in België de belangrijkste rechtsbron met betrekking tot medisch toezicht op werknemers. De relevante bepalingen staan opgenomen in Titel I, Hoofdstuk IV van deze Codex, en werden ingevoerd via het KB van 28 mei 2003 betreffende het gezondheidstoezicht van werknemers. Dit zogenaamde GezondheidstoezichtsKB¹¹ verplicht in artikel 26 en volgende bepaalde werknemers (onder meer in een veiligheidsfunctie, een functie met verhoogde waakzaamheid, een activiteit met welbepaald risico of een activiteit verbonden aan voedingswaren¹²) tot het ondergaan van een voorafgaand geneeskundig onderzoek.

¹¹ Koninklijk Besluit van 28 mei 2003 betreffende het gezondheidstoezicht op de werknemers, B.S. 16 juni 2003. Dit besluit werd geïncorporeerd in de zogenaamde Codex betreffende het welzijn op het werk, waarvan het hoofdstuk IV van Titel I uitmaakt.

¹² Voor een omschrijving van deze functies: zie artikel 2 van het GezondheidstoezichtsKB.

Het KB preciseert eveneens over welke onderzoeken het daarbij gaat, waarbij speciale aandacht moet uitgaan naar de mogelijkheid om te speuren naar afwijkingen en contra-indicaties met betrekking tot de geambeeerde post. Dit zou voor bepaalde functies bijvoorbeeld een alcohol- of drugtest kunnen verantwoorden, met een eventuele ongeschiktheidsverklaring door de onderzoekende arts tot gevolg. Deze diagnose mag evenwel niet worden opgenomen op het formulier voor de gezondheidsbeoordeling¹³, noch mag ze worden medegedeeld aan de werkgever¹⁴. De arbeidsgeneesheer mag de sollicitant enkel geschikt of ongeschikt verklaren, zonder aanvullende verklaringen. Tegen deze beslissing is geen verhaal mogelijk¹⁵.

Net als bij elk ander onderdeel van de sollicitatie heeft de sollicitant natuurlijk ook hier de mogelijkheid om zijn medewerking te weigeren. In dit geval kan de geneesheer niets anders doen dan de weigering mede te delen aan de werkgever, die hieraan vrij conclusies mag verbinden. De hierop veelal volgende afwijzing wordt in de regel niet aangemerkt als een fout in hoofde van de werkgever¹⁶.

Op die manier wordt een evenwicht gezocht tussen enerzijds de noodzaak om de medische geschiktheid van bepaalde sollicitanten te verzekeren en anderzijds het belang van de sollicitanten om hun privéleven optimaal af te schermen.

2) Medisch onderzoek op initiatief van de werkgever

Geheel anders is de situatie wanneer een medisch onderzoek niet wettelijk wordt verplicht, maar wanneer de werkgever zelf het initiatief neemt om een dergelijk onderzoek te organiseren als deel van de sollicitatieprocedure. Het wordt niet betwist dat de werkgever doorgaans een medisch onderzoek mag voorstellen aan aspirant-werknemers, noch dat zij hun deelname hieraan mogen weigeren. Aan de weigering mag echter enkel de afwijzing van een kandidaatsstelling worden verbonden wanneer het onderzoek van groot belang is om de geschiktheid voor de geëiseerde functie te beoordelen¹⁷.

Dit is een gevolg van artikel 11 van de hierboven besproken CAO nr. 38, dat stelt dat de persoonlijke levenssfeer van de sollicitant bij de wervingsprocedure moet worden geëerbiedigd. Dit artikel is onverminderd van toepassing bij medische onderzoeken, wat impliceert dat een medisch onderzoek enkel verantwoord is wanneer het relevant is omwille van de aard van de functie¹⁸.

Zo zou drug- of alcoholonderzoek toegelaten worden wanneer het gebruik van dergelijke middelen een gevaar zou opleveren voor collega's of derden¹⁹. Voor de meeste betrekkingen zal dit echter niet het geval

¹³ Artikel 48 van het Gezondheidstoezichtskb.

¹⁴ Artikel 24 van het Gezondheidstoezichtskb.

¹⁵ Artikel 59 van het Gezondheidstoezichtskb.

¹⁶ W. VAN EECKHOUTTE, "Juridische aspecten bij aanwerving", in X (ed), Privacy en andere grondrechten in de onderneming: naar een verantwoord ondernemingsbeleid?, Verslagen studiedag B.V.V.A. en Associare, Gent, 26 november 1993, 23; geciteerd in P. HUMBLET, I. PLETS en J.VANTHOURNOUT, Privacy van de werknemers, Kluwer, Mechelen, 2004, p.13.

¹⁷ Een zekere wettelijke grondslag voor deze opvatting vindt men ook in art. 14 van het Gezondheidstoezichtskb, dat stelt: "Tijdens de procedure van werving en selectie en tijdens de duur van de tewerkstelling mogen de werkgevers geen andere tests of medische onderzoeken laten uitvoeren dan deze die de preventieadviseur-arbeidsgeneesheer krachtens dit besluit mag uitvoeren, inzonderheid met een ander doel dan het staven van de beslissing dat de kandidaat of werknemer die onderworpen is aan de verplichte beoordeling van de gezondheid geschikt is in functie van de kenmerken van de betrokken werkpost of activiteit met welbepaald risico."

¹⁸ In die zin P. HUMBLET, I. PLETS en J.VANTHOURNOUT, Privacy van de werknemers, Kluwer, Mechelen, 2004, p.13.

¹⁹ Zie ook F.HENDRICKX, "Privacy en arbeidsrecht" in X (ed.), Brugge, Die Keure, 1999, p.236.

zijn, zodat een dergelijke maatregel in de meeste bedrijven geen veralgemeende praktijk of standaardprocedure zou mogen vormen.

Ook andere hierboven besproken gevolgen van het proportionaliteitsbeginsel (zoals het relatieve vraagrecht van de werkgever en de even relatieve spreekplicht van de sollicitant) gelden bij medische onderzoeken.

Bij deze testen worden doorgaans ook persoonsgegevens verwerkt, waardoor de Privacywet van toepassing is met alle hieraan verbonden gevolgen. Het voornaamste gevolg is wellicht dat de werkgever verplicht is de sollicitant op de hoogte te brengen van de draagwijdte en het doel van het onderzoek (artikel 9 van de Privacywet). Dit resulteert in de praktijk frequent in het aflassen van het onderzoek, vermits een sollicitant met gezondheidsproblemen veelal vooraf zal afhaken wanneer hij te horen krijgt dat zijn medische toestand zal worden onderzocht.

Indien een kandidaat wordt afgewezen op grond van de bevindingen die voortvloeien uit een medisch onderzoek, dan zal de afwijzing bijzonder grondig moeten worden gemotiveerd. Immers, de vaststelling van een gezondheidsprobleem kan nooit automatisch leiden tot de uitsluiting van een kandidaat. Er zal steeds moeten worden aangetoond dat het probleem resulteert in een functionele ongeschiktheid voor de betrekking in kwestie.

Zo volgt uit een positieve cannabistest niet noodzakelijkerwijze de ongeschiktheid van een kandidaat. Cannabis kan immers nog weken na occasioneel gebruik worden opgespoord, zodat niet per definitie kan worden besloten dat de sollicitant arbeidsongeschikt is. De aard van de functie speelt hierbij een grote rol: van een vrachtwagenchauffeur zal men sneller een volledig zuivere medische achtergrond kunnen eisen dan van bijvoorbeeld een administratieve bediende.

Voor specifieke categorieën van gezondheidsonderzoeken moet men bovendien rekening houden met de wet van 28 januari 2003 betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd²⁰. De wet is zowel van toepassing op sollicitanten, bestaande werknemers als statutaire werknemers, en is bedoeld om te vermijden dat de werkgever hun geschiktheid voor een bepaalde positie beoordeelt aan de hand van voorspellend genetisch onderzoek of aidstests. Het is belangrijk op te merken dat de wet niet alleen van toepassing is bij sollicitatiegesprekken, maar ook bij beslissingen over de toekenning van een functie aan een bestaande werknemer (bijvoorbeeld bij promotie of overstap naar een ander departement).

Artikel 3 van de wet bevestigt het principe dat biologische tests of medische onderzoeken niet per definitie verboden zijn, maar dat zij enkel toelaatbaar zijn voor de beoordeling van de huidige geschiktheid van de werknemer voor de openstaande betrekking. Voorspellend genetisch onderzoek en een aidstest worden daarbij in beginsel²¹ verboden. Bovendien moet de (kandidaat-)werknemer 10 dagen voor het onderzoek bij een vertrouwelijke en aangetekende brief worden verwittigd van de precieze modaliteiten en doeleinden van het onderzoek. De werkgever moet hem ook meedelen welke gezondheidsproblemen zouden kunnen

²⁰ Wet van 28 januari 2003 betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd, B.S. 9 april 2003

²¹ Artikel 5 van de wet laat de Koning toe om uitzonderingen te maken. In het kader van deze tekst gaan we hierop niet verder in.

verergeren ten gevolge van de uitoefening van de betrekking.

Wanneer de preventieadviseur-arbeidsgeneeskunde na het onderzoek besluit tot ongeschiktheid van de kandidaat dient hij deze beslissing schriftelijk en gemotiveerd over te maken aan een arts die door de (kandidaat-)werknemer werd aangeduid, op straffe van nietigheid. De werkgever en de kandidaat moeten eveneens op de hoogte worden gebracht middels een fiche van medisch onderzoek.

Personeelsbeheer en algemene administratie

Ook – en zelfs in het bijzonder – na het aangaan van de arbeidsrelatie zal de werkgever verplicht zijn bepaalde persoonlijke gegevens met betrekking tot de werknemers te bewaren. Het gaat onder meer om het aanmaken en onderhouden van personeelsfiches, prestatie-evaluaties, loonbeheer en dergelijke administratieve taken. Het zal duidelijk zijn dat deze gegevens veelal persoonsgegevens zijn in de zin van de Privacywet, en dat de meeste bewerkingen van deze gegevens moeten worden beschouwd als verwerkingen volgens dezelfde wet. De voorwaarden en verplichtingen van de Privacywet moeten in principe dan ook worden nageleefd.

Hieronder bespreken we kort de voornaamste gevolgen van deze principiële toepasselijkheid. Hoewel er een aantal (uitzonderings)bepalingen op maat van de arbeidsrelatie zijn geschreven gaat het meestal om abstracte regels die in de praktijk moeten worden geapprecieerd. Gedragscodes kunnen hierbij een nuttig hulpmiddel zijn, waarbij in het bijzonder kan worden verwezen naar de Gedragscode van de Internationale Arbeidsorganisatie met betrekking tot de bescherming van de persoonsgegevens van werknemers²². Deze code, die in 1996 werd goedgekeurd, heeft weliswaar geen juridische bindende kracht, maar kan desondanks een hulpmiddel zijn bij de interpretatie van de toepasselijke wettelijke bepalingen.

Toestemming en noodzaak

Elke verwerking van persoonsgegevens moet gebaseerd zijn op hetzij de toestemming van de betrokkene, hetzij op een bepaald belang dat zwaarder weegt dan het gebrek aan een toestemming (artikel 5 Privacywet).

Dit vereiste levert in feite weinig problemen op. Op de eerste plaats kan worden gezegd dat de werknemer zijn ondubbelzinnige toestemming geeft voor de verwerking van zijn persoonsgegevens door het aangaan van een arbeidsrelatie. Maar ook wanneer deze hypothese wordt verworpen zijn er een aantal rechtsgronden waarop de werkgever zich kan beroepen. Zo kan onder meer worden geargumenteed dat een verwerking van persoonsgegevens noodzakelijk is voor de uitvoering van een arbeidsovereenkomst (artikel 5, b), of

²² On line beschikbaar via de website van de IAO:
<http://www.ilo.org/public/english/support/publ/pdf/protect.pdf>

dat de werkgever een gerechtvaardigd belang heeft bij de verwerking dat zwaarder doorweegt dan de hieruit resulterende privacyinbreuk bij de betrokkene (artikel 5, f).

Hoe dan ook levert de vereiste toestemming/noodzaak nagenoeg nooit discussies op.

Finaliteit en geoorloofd karakter

De werkgever is in principe verplicht de werknemer te informeren over de doeleinden van de verwerkingen die hij zal doorvoeren. Daarna is elke verdere verwerking geoorloofd die verzoenbaar is met de aangegeven doeleinden, in het bijzonder rekening houdend met de legitieme verwachtingen van de werknemer (artikel 4, 2° van de Privacywet). Voor zover het algemene administratiegegevens betreft (zoals loonsadministratie, fiscale gegevens, opleiding, CV's) stelt dit weinig problemen, vermits dit veelal verwerkingen zijn die binnen de normale verwachtingen van een werknemer vallen.

Voor een aantal meer controversiële verwerkingen is dit echter niet het geval, waarbij onder meer gedacht kan worden aan de registratie van communicatiegegevens, gezondheidsgegevens en informatie die bestemd is voor de evaluatie van de werknemer. Ook in deze gevallen blijft de Privacywet van toepassing, zij het dat de wetgever in een aantal gevallen in specifiekere wettelijke verplichtingen heeft voorzien. We kunnen hier onder meer verwijzen naar de hierboven besproken regeling voor sollicitaties en medisch toezicht, en de hieronder besproken regeling voor camera- en telecommunicatietoezicht op de werknemers.

Informatieverplichting

Ook hier worden de verplichtingen van de werkgever voorgeschreven door de Privacywet (artikel 9). Dit komt er veelal op neer dat de werknemer moet worden geïnformeerd over de aard en de omvang van de gegevens die de werkgever over hem bijhoudt. Meestal zal aan deze verplichting worden voldaan via de arbeidsovereenkomst, het arbeidsreglement of sectoriële mededelingen, voor zover de wet geen ander kenbaarmakingsmechanisme inbouwt.

Gegevenscategorieën en proportionaliteit

Artikel 4, 3° van de Privacywet stelt voorop dat elke verwerking van persoonsgegevens "toereikend, terzake dienend en niet overmatig [moet] zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt." Voor werkgevers impliceert dit met name dat hun algemene administratie enkel gegevens mag bevatten die relevant zijn voor het personeelsbeheer en dat deze gegevens enkel mogen worden verwerkt indien dit noodzakelijk is voor de goede werking van het bedrijf.

Ook hier kunnen er zich vooral problemen stellen voor een aantal aparte gegevenscategorieën, zoals gezondheidsgegevens en telecommunicatiegegevens. Voor deze gegevens heeft de wetgever veelal in aparte regelgeving voorzien, die elders in dit hoofdstuk wordt besproken.

Zoals ook al werd aangehaald in hoofdstuk I heeft de Privacywet zelf eveneens voorzien in een bijkomende bescherming voor een aantal gegevenscategorieën in artikel 6 t/m 8 van de Privacywet, zoals voor:

- gegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, evenals persoonsgegevens die het seksuele leven betreffen;
- persoonsgegevens die de gezondheid betreffen;
- persoonsgegevens in verband met geschillen voorgelegd aan hoven en rechtbanken of aan administratieve gerechten inzake verdenkingen, vervolgingen of veroordelingen met betrekking tot misdrijven, of inzake administratieve sancties of veiligheidsmaatregelen.

De verwerking van deze gegevens is in principe verboden. Hierop bestaan een aantal uitzonderingen, waarvan voor werkgevers de belangrijkste is dat de eerste twee categorieën van beschermde gegevens wel mogen worden verwerkt “wanneer de verwerking noodzakelijk is met het oog op de uitvoering van de specifieke verplichtingen en rechten van de verantwoordelijke voor de verwerking met betrekking tot het arbeidsrecht”.

Met uitzondering van gerechtelijke gegevens zal ook voor deze gegevenscategorieën de verwerking dus toch veelal toegelaten zijn – zelfs zonder de aparte toestemming van de werknemer – wanneer dit noodzakelijk is op grond van de arbeidsrechtelijke verhouding. In feite komt dit neer op een herformulering van de criteria van artikel 8 van het EVRM: als de verwerking legitiem, legaal en proportioneel is (wat ook impliceert dat zij niet strijdig is met andere specifieke wetgeving), dan is zij geoorloofd.

Ten slotte moet nog worden opgemerkt dat, net zoals in elke andere context, het proportionaliteitscriterium ook vereist dat gegevens enkel mogen worden bewaard zolang zij een legitiem nut hebben voor de werkgever. Persoonsgegevens van werknemers die geen verder nut meer kunnen hebben (wat het geval kan zijn wanneer enige tijd is verstreken na het ontslag of overlijden van een werknemer) moeten daarom worden gewist, of minstens geanonimiseerd.

Aangifte bij de Privacycommissie

Alvorens persoonsgegevens op een geheel of gedeeltelijk geautomatiseerde manier mogen worden verwerkt – wat meestal het geval is bij personeels- en klantenbeheer en loonadministratie – moeten de geplande verwerkingen in principe worden aangegeven bij de Belgische Privacycommissie op grond van artikel 17 van de Privacywet. Het is duidelijk dat dit voor nagenoeg elke Belgische werkgever het geval zou zijn, zodat de Commissie overspoeld zou worden door aangiften van verwerkingen die in hoofddorde weinig privacygevoelig zijn.

Om die reden voorziet het Koninklijk besluit tot uitvoering van de Privacywet²³ in artikel 51 en volgende in een aantal uitzonderingen op de aangifteverplichting. Vanuit arbeidsrechtelijk standpunt²⁴ zijn artikel 51 en 52 de belangrijkste bepalingen.

Deze artikelen bevatten een vrijstelling van de aangifteplicht voor verwerkingen van persoonsgegevens die uitsluitend betrekking hebben loonadministratiegegevens²⁵ (artikel 51) of algemene personeelsadministratie²⁶ (artikel 52). De vrijstellingen gelden enkel voorzover het gaat om het eigen personeel van de verantwoordelijke voor de verwerking (meestal de werkgever), en enkel wanneer de gegevens uitsluitend voor dit doel worden gebruikt.

Ook de mededeling aan derden is streng gereguleerd: loonadministratiegegevens mogen alleen worden meegedeeld aan de ontvangers die daartoe gerechtigd zijn, en personeelsadministratiegegevens mogen zelfs enkel worden overgedragen in het kader van de toepassing van een wets- of verordeningsbepaling of indien nodig voor de verwezenlijking van de doelstellingen van de verwerking. Personeelsadministratiegegevens mogen bovendien geen betrekking hebben op gevoelige gegevens die een bijzondere wettelijke bescherming genieten, of op gegevens die bestemd zijn voor de evaluatie van de betrokken persoon.

Medische controle tijdens de arbeid

Hierboven gingen we reeds dieper in op de toepasselijke bepalingen bij het aangaan van een arbeidsrelatie, m.a.w. tijdens wervings- en selectieprocedures. Vermits de lichamelijke gezondheid van de werknemer van groot belang is voor zijn productiviteit spreekt het voor zich dat de werkgever er een belang bij heeft om zijn gezagsuitoefening ook uit te strekken tot medische controles. Men kan zich de vraag stellen of dit de werkgever het recht geeft om een medische controle af te dwingen.

Naast de gezagsuitoefening lijkt er nog een tweede mogelijke verantwoordingsgrond voor een verplichte medische controle te zijn. Artikel 20, 2° van de Arbeidsovereenkomstenwet stelt immers dat:

“De werkgever is verplicht [...] als een goed huisvader te zorgen dat de arbeid wordt verricht in behoorlijke omstandigheden met betrekking tot de veiligheid en de gezondheid van de werknemer en dat hem bij een ongeval de eerste hulpmiddelen verstrekt kunnen worden. Te dien einde moet een verbandkist voortdurend ter beschikking van het personeel zijn.”

Hoewel het artikel duidelijk vooral op maat van de reactieve gezondheidszorg is geschreven (m.a.w. de werkgever moet er zorg voor dragen dat de nodige middelen voorhanden zijn om zieke of gekwetste werknemers de nodige eerste hulp te verlenen) kan in dit artikel ook een verplichting worden gelezen om de gezondheid van de werknemer in het algemeen te behartigen. De verplichting om een preventie- en beschermingsbeleid te voeren zou dan de grondslag zijn voor een controlerecht van de werkgever.

²³ Koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, B.S. 13 maart 2001

²⁴ Andere gedeeltelijke vrijstellingen betreffen klantenbeheer, leveranciersbeheer en administratie van aandeelhouders en vennoten.

²⁵ Het gaat om loonadministratie in de ruime zin, wat alle vormen van vergoedingen en compensaties dekt, en ongeacht het statuut van de beneficiaris (werknemer, stagair, zelfstandige, ...). Alle hiervoor relevante gegevens komen in aanmerking voor de vrijstelling: identificatiegegevens, financiële details, gezinssamenstelling, opleiding, achtergrond, CV's,...

²⁶ Het gaat om elke verwerking die betrekking heeft op de werknemers en die niet rechtstreeks voortvloeit uit de toepasselijke wettelijk, reglementaire of conventionele bepalingen. Dit dekt onder meer selectie en recruitering, trainingsopportuniteiten, loopbaanplanning en dergelijke meer.

Nochtans stelt de rechtspraak zich hier streng op, en wordt in het algemeen het standpunt ingenomen dat na de aanwerving de werknemer niet verplicht kan worden om zijn arbeidsgeschiktheid middels een medische test aan te tonen. Het Hof van Cassatie heeft dit standpunt overigens al meermaals²⁷ expliciet bevestigd.

Zelfs wanneer de werknemer akkoord gaat met een medische controle blijven bepaalde onderzoeken verboden. In het bijzonder kunnen we verwijzen naar de hierboven reeds besproken wet van 28 januari 2003 betreffende de medische onderzoeken die binnen het kader van de arbeidsverhoudingen worden uitgevoerd. Vermits deze wet ook van toepassing is bij beslissingen over de toekenning van een functie aan een bestaande werknemer (bijvoorbeeld bij promotie of overstap naar een ander departement) zijn ook hier voorspellend genetisch onderzoek en een aidstest in beginsel verboden.

Een bijzondere toepassing hiervan is het gebruik van drugs-en alcoholcontroles op de werkplaats, waar men zou kunnen denken dat de werkgever een zware bewijslast torst indien hij geen gebruik mag maken van medische tests om een actueel probleem aan te tonen. Nochtans steunt dit standpunt op een misvatting: hoewel de vaststelling van een intoxicatie weliswaar in het verkeersrecht zeer belangrijk is, is dit in het arbeidsrecht niet noodzakelijk het geval. Indien men een werknemer wenst te ontslaan omwille van dringende redenen, met name alcohol-of drugsmisbruik die een invloed heeft op de werkprestaties, dan hoeft men de aanwezigheid van een exacte hoeveelheid van bepaalde stoffen in het lichaam van de betrokkene immers niet aan te tonen.

Het is met andere woorden niet nodig om de adem, de urine of het bloed van de werkgever te analyseren teneinde een bepaalde hoeveelheid intoxicerende stoffen aan te treffen.

Het volstaat om vast te stellen dat de werknemer niet meer in staat is om zijn functie op een normale wijze uit te oefenen²⁸. Dit impliceert echter ook dat een werknemer die wel geïntoxiceerd is (in die zin dat er sporen van drugs of alcohol in zijn lichaam terug te vinden zijn) geen aanleiding tot zijn ontslag geeft indien hij desondanks op de gepaste manier zijn werk kan uitvoeren en geen gevaar voor zijn medewerkers betekent. Medische testen om drug- of drankmisbruik vast te stellen zijn dus niet alleen juridisch betwistbaar, maar in de praktijk ook slechts beperkt nuttig²⁹.

Op het principiële verbod op verplichte medische controles in een arbeidsverhouding bestaat er één duidelijke uitzondering, namelijk wanneer de werknemer zelf volhoudt arbeidsongeschikt te zijn omwille van medische redenen.

In die hypothese bestaat er immers een expliciete wettelijke grondslag voor een medische controle. De Arbeidsovereenkomstenwet bevat een regeling voor arbeidsongeschiktheid ten gevolge van ziekte of ongeval, waarbij (een deel van) de kosten die voortvloeien uit de ongeschiktheid ten laste van de werkgever vallen. Als tegenhanger van deze verplichting kent artikel 31, §3 de werkgever het recht toe een medische controle door een bedrijfsarts op te leggen. De werknemer mag deze controle niet weigeren. In geval van

²⁷ Cass. 11 maart 1985, J.T.T. 1985, 286, noot C. WANTIEZ; Cass. 15 februari 1973, T.S.R. 1974, 28.

²⁸ Ingeval van dronkenschap wordt er vaak verwezen naar de omschrijvingen die onder invloed van het Hof van Cassatie tot stand zijn gekomen: de werknemer moet zodanig onder invloed zijn van de drank dat hij geen bestendige controle over zijn handelingen meer heeft, zonder daarom noodzakelijk het zelfbewustzijn van deze daden te hebben verloren. Cass. 6 maart 1956, Pas. 1956, I, 789; Cass. 27 mei 1957, R.W. 1957-58, 1151; Cass. 8 augustus 1958, Pas. 1959, I, 361; Cass. 16 februari 1971, Arr. Cass. 1971, 581; Cass. 24 april 1974, Arr.Cass. 1974, 916.

²⁹ Zie voor een uitgebreid overzicht van deze problematiek P. HUMBLET, I. PLETS en J.VANTHOURNOUT, *Privacy van de werknemers*, Kluwer, Mechelen, 2004, p.16 en volgende.

betwistingen over de ongeschiktheid kunnen beide partijen de tussenkomst van een arts-scheidsrechter vorderen. Wanneer de werknemer claimt om medische redenen arbeidsongeschikt te zijn, dan kan een medische controle dus worden opgelegd³⁰.

Daarnaast moet er ook rekening worden gehouden met de bepalingen van de Codex over het welzijn op het werk. Net als bij het sollicitatiegesprek (hierboven reeds besproken) verplicht het GezondheidstoezichtsKB³¹ in artikel 30 en volgende tot de organisatie van een zeker periodiek medisch toezicht op bepaalde categorieën van werknemers (onder meer in een veiligheidsfunctie, een functie met verhoogde waakzaamheid, een activiteit met welbepaald risico of een activiteit verbonden aan voedingswaren³²). In principe is de werkgever verplicht deze onderzoeken te verrichten, en mogen de werknemers er zich niet aan onttrekken.

Artikel 4 van dit KB verplicht de werkgever om “de nodige maatregelen te nemen opdat deze werknemers verplicht onder gezondheidstoezicht staan, en opdat de uitvoering van dit gezondheidstoezicht verloopt overeenkomstig de voorschriften van dit besluit.” Dit impliceert niet dat hij dit toezicht zelf moet organiseren; maar enkel dat hij moet verifiëren dat het toezicht reël bestaat. Het toezicht is niet verplicht wanneer uit een voorafgaande risicoanalyse, uitgevoerd volgens de modaliteiten van het KB, blijkt dat dit niet nodig is.

Wanneer een werknemer verplicht is om zich aan een medische controle te onderwerpen maar dit weigert, dan mag de werkgever hem niet aan het werk houden. In de praktijk impliceert dit meestal dat een standvastige weigering van de werknemer om zich aan een verplicht onderzoek te onderwerpen aanleiding kan geven tot een ontslag om dringende redenen, zonder dat er sprake is van een fout in hoofde van de werkgever.

Overigens is de werkgever niet alleen verplicht om deze categorieën werkgevers aan een verplichte controle te onderwerpen, maar moet hij krachtens artikel 5 van het GezondheidstoezichtsKB er ook voor zorgen “dat elke werknemer die dit wenst op gezette tijden van een gezondheidstoezicht kan genieten betreffende de risico’s voor zijn veiligheid en gezondheid op het werk.” In dit geval gaat het dus niet om een verplichte controle, maar moet het gewoon mogelijk zijn om een medische controle te regelen voor werknemer die dit op eigen beweging vragen.

Op die manier wordt een evenwicht gezocht tussen enerzijds de noodzaak om de medische geschiktheid van bepaalde sollicitanten te verzekeren en anderzijds het belang van de sollicitanten om hun privéleven optimaal af te schermen.

³⁰ Zie onder meer PWATRIN, Medische controle van de arbeidsongeschiktheid in het kader van de Wet van 3 juli 1978, Diegem, ced.samsom, 1993, 17.

³¹ Koninklijk Besluit van 28 mei 2003 betreffende het gezondheidstoezicht op de werknemers, B.S. 16 juni 2003. Dit besluit werd geïncorporeerd in de zogenaamde Codex betreffende het welzijn op het werk, waarvan het hoofdstuk IV van Titel I uitmaakt.

³² Voor een omschrijving van deze functies: zie artikel 2 van het GezondheidstoezichtsKB.

Videobewaking en webcams

De steeds verder toenemende penetratie van nieuwe technologieën laat op technologisch vlak ook een steeds verregaander toezicht op de werknemers toe. Zowel camera's als opslagmedia worden immers steeds goedkoper, zodat er op technologisch vlak nog weinig beperkingen zijn aan de omvang van de gezagsuitoefening. De werkgever zou desgewenst zijn werknemers nagenoeg constant kunnen observeren en hun gedrag vastleggen voor latere controle. Op die manier kunnen onproductieve of contraproductieve werknemers worden geïdentificeerd en eventueel verwijderd.

Dat dergelijke systemen ook een bredere toepassing krijgen kan men vaststellen in het advies van de Privacycommissie van 12 april 2006³³ in verband met het gebruik van webcams in kindercrèches. De Commissie stelde vast dat een aantal crèches was begonnen met het installeren van webcams, zodat bezorgde ouders op vaste momenten via het internet het wel en wee van hun kroost zouden kunnen volgen. Op die manier konden zij niet alleen nagaan of de zorgverstrekkers hun plicht op een gepaste wijze deden, maar ook waarmee hun kinderen zich zelf onledig hielden. Dergelijke systemen stoten natuurlijk op talloze bezwaren: de gebruikers van de websites kunnen immers alle kinderen in de gaten houden, ongeacht enige familiale band of toestemming van de ouders, en bovendien kunnen zij ook elke andere persoon die toevallig in beeld zou komen surveilleren, zoals het personeel van de crèche of eventuele derden. De Privacycommissie adviseerde dan ook negatief, en stelde dat dergelijke monitoringssystemen als disproportioneel moesten worden aangemerkt.

In dit advies lag de nadruk op de rechten van het kind en op de (eventueel geschade) keuzevrijheid van de ouders als vertegenwoordigers van het kind. Men kan zich echter ook de vraag stellen in welke mate een dergelijke systematisch toezicht verzoenbaar is met het recht op privacy van de werknemers, en of dit niet manifest de grenzen overschrijdt van wat als een normale gezagsuitoefening kan worden beschouwd. Om een leidraad te bieden voor het beantwoorden van deze vraag keurde de NAR op 16 juni 1998 CAO 68 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats³⁴ goed. Deze CAO werd algemeen verbindend verklaard bij KB van 20 september 1998.

Bovendien werd op 21 maart 2007 de Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's (de Camerawet) goedgekeurd. Ook deze wet kan van toepassing zijn in een arbeidscontext, bijvoorbeeld wanneer camera's worden geplaatst zowel om toezicht te houden op de werknemers als om veiligheidsincidenten te voorkomen. De draagwijdte van deze wet werd reeds toegelicht in Hoofdstuk 4; en de bespreking hieronder zal zich dan ook voornamelijk toeleggen op CAO 68.

Deze CAO is een verbijzondering van de hierboven besproken Privacywet. Immers, het maken van cameraopnamen met de bedoeling om individuele werknemers systematisch te kunnen identificeren moet

³³ Zie http://www.privacycommission.be/nl/docs/Commission/2006/advies_08_2006.pdf; laatst bezocht op 26 augustus 2008.

³⁴ Collectieve arbeidsovereenkomst nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats (algemeen verbindend verklaard door het KB van 20 september 1998, B.S. 2 oktober 1998).

worden beschouwd als een verwerking van persoonsgegevens³⁵, zodat de voorwaarden van de Privacywet in deze hypothese moeten worden nageleefd. De CAO specificeert op welke wijze dit kan gebeuren met betrekking tot camerabewaking, ongeacht of het beeldmateriaal wordt opgeslagen of enkel live wordt bekeken (bijvoorbeeld door een bewakingsdienst).

Aanvankelijk had de CAO een bredere draagwijdte dan de Privacywet, die volgens de Privacycommissie immers enkel van toepassing was als de beelden ook werden bewaard³⁶. Na de aanpassing van de Privacywet in 1998 verloor dit criterium zijn belang, en bevestigde de Privacycommissie dat de Privacywet ook van toepassing is indien het materiaal niet wordt opgeslagen³⁷. Het toepassingsgebied van de CAO en de Privacywet valt in die zin dus voor een groot deel samen.

Finaliteits- en proportionaliteitsprincipe

De artikelen 4 tot en met 8 van CAO 68 bepalen aan welke finaliteits- en proportionaliteitsvereisten camerabewaking op een arbeidsplaats moeten voldoen.

Op de eerste plaats laat artikel 4, §1 camerabewaking enkel toe wanneer dit gebeurt omwille één van vier expliciet opgenoemde doeleinden:

- de bescherming van de veiligheid en gezondheid van de werknemers (bijvoorbeeld camerabewaking in een chemische opslagplaats);
- de bescherming van de goederen van de onderneming (bijvoorbeeld als bescherming tegen diefstal door werknemers);
- de controle van het productieproces (bijvoorbeeld een camera die een lopende band en/of de daaraan werkende personen in de gaten houdt³⁸); of

³⁵ Zie het advies van de Privacycommissie van 7 juni 1995 betreffende de toepasselijkheid van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens op beeldopnamen, en de gevolgen ervan: "Visuele beelden zijn gegevens in de zin van de [Privacywet]. Indien zij betrekking hebben op één of meerdere natuurlijke personen die geïdentificeerd zijn of kunnen worden, zijn zij bovendien persoonsgegevens in de zin van de [Privacywet] (zie de verklaring van de Minister van Justitie tijdens de bespreking van het ontwerp dat geleid heeft tot de Wet Verwerking Persoonsgegevens, verslag Vandenbergh, Parl.St., Senaat, B.Z. 1991-92, nr. 445-2, p. 57). Een persoon kan als niet-identificeerbaar worden beschouwd wanneer het identificatieproces onredelijke inspanningen of kosten vergt in verhouding tot het nut ervan. [...] In het licht van het voorgaande dienen beelden van personen niet als persoonsgegevens in de zin van de Wet Verwerking Persoonsgegevens te worden beschouwd, indien zij niet systematisch worden gebruikt om de personen te identificeren. [...] Anders wordt het wanneer deze beelden specifiek opgenomen worden met de bedoeling, bijvoorbeeld in het kader van het bewaken van de veiligheid, om de opgenomen personen te kunnen identificeren.

³⁶ Zie het advies van de Privacycommissie van 7 juni 1995 betreffende de toepasselijkheid van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens op beeldopnamen, en de gevolgen ervan: "Er is sprake van een verwerking van beelden in de zin van de Wet Verwerking Persoonsgegevens zodra de beelden niet alleen worden opgenomen en onmiddellijk weergegeven, maar ook worden bewaard. Observatiesystemen waarbij de beelden niet worden bewaard, vallen niet onder het toepassingsgebied van de Wet Verwerking Persoonsgegevens."

³⁷ Zie het advies van de Privacycommissie van 13 december 1999 betreffende de verwerkingen van beelden, in het bijzonder verricht door middel van systemen van video-toezicht: "De wet van 11 december 1998 bracht wijzigingen in het wettelijk kader aan. Het is niet meer noodzakelijk dat de gegevens bewaard worden opdat er sprake is van een verwerking, dus bijgevolg ook niet dat de verwerking geautomatiseerd is (nieuwe artikelen 1, §2 en 3). De verzameling op zich is immers een verwerking. De bewaring van de opgenomen gegevens is dus geen noodzakelijke voorwaarde meer voor de toepassing van de wet: deze is van toepassing vanaf het moment dat de beelden gefilmd worden."

³⁸ Artikel 4 expliciteert dat de controle van het productieproces betrekking kan hebben op zowel de machines als op de werknemers. Zij kan dus zowel dienen om de goede werking van de machines na te gaan als om de werkorganisatie te evalueren en te verbeteren. Het onderscheid is niet altijd eenvoudig te maken, aangezien bij camerabewaking van het productieproces veelal zowel de werknemers als de machines in beeld zullen komen. De commentaren bij artikel 6 van de CAO lijken voorop te stellen dat er enkel sprake is van camerabewaking van machines wanneer "het niet de bedoeling is om de werknemer te viseren". De intentie en de doelgerichtheid van het bewakingsproces lijken dus de doorslaggevende elementen te zijn.

- de controle van de arbeid van de werknemer (bijvoorbeeld om de productiviteit van de personeelsleden te controleren). Beslissingen en beoordelingen door de werkgever mogen nooit enkel gebaseerd worden op gegevens die via camerabewaking om dit doeleinde verkregen werden.

Het gaat om breed geformuleerde criteria, die nagenoeg steeds van toepassing kunnen zijn. Om die reden verplicht §2 van artikel 4 de werkgever om het doeleinde van de camerabewaking duidelijk en expliciet te omschrijven. Deze informatie moet voorafgaand aan de inwerkingstelling van het toezicht worden bekendgemaakt, zoals hieronder zal worden beschreven.

Voor de beoordeling van de legitimiteit van de camerabewaking moet er voorts rekening mee worden gehouden of de camerabewaking tijdelijk, dan wel voortdurend is. Tijdelijke bewaking – waarbij er m.a.w. ook onbewaakte periodes op de arbeidsplaats zijn – is vanzelfsprekend minder indringend en zal dus ook sneller worden toegelaten.

Voor alle vier de hierboven vermelde doeleinden kan tijdelijke camerabewaking geoorloofd zijn. Permanente bewaking is echter enkel toegelaten ter bescherming van de van de veiligheid en gezondheid, de bescherming van de goederen van de onderneming, of de controle van het productieproces die enkel betrekking heeft op de machines.

Louter de controle van de arbeid van de werknemer of van het functioneren van de werknemer in het productieproces kan dus nooit een permanente bewaking verantwoorden.

Net als bij de Privacywet legt ook CAO 68 vast dat de camerabewaking (die tenslotte ook een verwerking van persoonsgegevens kan zijn) niet mag worden aangewend op een wijze die onverenigbaar is met het uitdrukkelijk omschreven doeleinde. Met andere woorden: de werkgever (de verwerker) moet één of meerdere van de exhaustief opgesomde doeleinden expliciet kenbaar maken, en elk verder gebruik van de bewaking moet hiermee verzoenbaar zijn en te goeder trouw (artikel 13).

Worden de verkregen beelden gebruikt voor dergelijke verzoenbare doeleinden, dan moet de werkgever ervoor zorgen dat alle maatregelen genomen worden om interpretatiefouten te vermijden. De bewaking moet bovendien, uitgaande van dit doeleinde, toereikend, ter zake dienend en niet overmatig zijn. Op die manier weet de werknemer waaraan hij zich mag verwachten.

De vereiste proportionaliteit van het toezicht blijkt ook uit artikel 8, dat bepaalt dat de camerabewaking in principe geen inmenging in de persoonlijke levenssfeer van de werknemer tot gevolg mag hebben. Indien een dergelijke inmenging onvermijdelijk is, dan moet zij tot een minimum beperkt worden.

Procedurevoorwaarden: informatie en consultatie

Ook voor wat betreft de informatie-uitwisseling is de CAO een getrouwe weerspiegeling van de vereisten van de Privacywet. Wanneer de bewakingsmaatregelen een inbreuk dreigen te vormen op de persoonlijke levenssfeer van de werknemers, dan is de werkgever niet alleen gehouden tot het informeren van zijn personeel (artikel 9), maar ook tot een consultatie van hun vertegenwoordigers.

1) Informatieverstrekking aan de werknemers

De geprivilegieerde gesprekspartner bij de invoering van camerabewaking is de ondernemingsraad. Deze moet voordat de bewaking wordt ingesteld op de hoogte worden gebracht³⁹ van het doeleinde, de vraag of het beeldmateriaal al dan niet bewaard wordt, het aantal en de plaatsing van de camera('s), en de geplande observatieperiodes. Beschikt de onderneming niet over een ondernemingsraad, dan wordt het comité voor preventie en bescherming op het werk geïnformeerd of, bij ontstentenis daarvan, de vakbondsafvaardiging of ten slotte bij ontstentenis daarvan: de werknemers zelf. Er wordt met andere woorden getracht de informatie te richten op het minst kwetsbare professionele niveau binnen de onderneming. Dit moet ertoe leiden dat er niet enkel eenzijdig informatie wordt verstrekt, maar dat de betrokken partijen een actieve dialoog aangaan.

De voorafgaande informatieverstrekking aan de vertegenwoordigingsorganen is echter onvoldoende: de werkgever is eveneens steeds verplicht om dezelfde informatie rechtstreeks te verstrekken aan de betrokken werknemers bij het opstarten van de camerabewaking.

Nochtans heeft het Hof van Cassatie het onlangs nodig geacht te verduidelijken dat er situaties bestaan waarin deze regel niet van toepassing is. In een arrest van 2 maart 2005⁴⁰ steunde het Hof het standpunt van een werkgever die één van zijn werknemers verdacht van diefstal, en daarom een camera bij de kassa's plaatste zonder zijn personeel hierover in te lichten. De vermoedens bleken gegrond: de beelden toonden duidelijk aan dat de verdachte kassierster inderdaad een deel van de inhoud bleek te ontvreemden, en zij werd op basis van deze beelden dan ook op slaande voet ontslagen wegens dringende reden.

Vermits de beelden werden verkregen in strijd met de bepalingen van CAO 68 argumenteerde de kassierster dat het ging om onrechtmatig verkregen bewijs, en dat haar ontslag foutief was. Verrassend genoeg volgde het Hof dit standpunt niet. De camera werd immers slechts geplaatst nadat er een gegronde reden was om diefstal te vermoeden, en bovendien lette de werkgever erop dat enkel de activiteiten van de verdachte kassierster werden opgenomen (en dus niet bv. de handelingen van andere collega's). In dit concrete geval oordeelde het Hof dat de werkgever de nodige maatregelen had genomen om de inbreuk op de persoonlijke levenssfeer van de werknemers tot een absoluut minimum te beperken, en dat de maatregel daarom geoorloofd was.

Het gaat om een enigszins verwonderlijk oordeel, omdat de voorschriften van de CAO vrij flagrant werden genegeerd. Men zou daarom kunnen⁴¹ verwachten dat het Hof van Cassatie zou besluiten dat het onrechtmatig verkregen bewijsmateriaal had moeten worden geweerd. Toch kan er begrip worden opgebracht voor het standpunt van het Hof. De CAO is immers bestemd om de persoonlijke levenssfeer te beschermen tegen inbreuken, maar deze bescherming is niet absoluut. Zij zou zeker niet voor gevolg mogen hebben dat strafbare feiten onvervolgbaar worden doordat de dader de facto beschermd wordt tegen elke verkrijging van bewijsmateriaal.

³⁹ De exacte te volgen procedure wordt in artikel 9 van de CAO uitgewerkt, maar zal hier niet verder in detail worden bekeken.

⁴⁰ Cass. 2 maart 2005, n.gepubl., on-line beschikbaar via www.juridat.be.

⁴¹ Dit traditionele standpunt werd in een reeks arresten van het Hof van Cassatie sinds 2003 steeds verder uitgehouden. Van bijzonder belang is het arrest van 14 oktober 2003. Dit arrest stelt dat de omstandigheid dat een bewijselement op onrechtmatige wijze is verkregen niet ipso facto de uitsluiting ervan tot gevolg heeft. Dit zou alleen maar het geval zijn (1) wanneer een op straffe van nietigheid voorgeschreven vormvereiste wordt miskend; (2) wanneer de onregelmatigheid de betrouwbaarheid van het bewijs aantast; (3) wanneer het gebruik van het bewijs in strijd is met het recht op een eerlijk proces. Volgens het Hof was hiervan in dit geval geen sprake.

Klaarblijkelijk oordeelde het Hof dat de schending van de CAO door de werkgever in dit geval niet even zwaar woog als het misdrijf van de kassierster, en dat de inbreuk op de persoonlijke levenssfeer van de verdachte geoorloofd was. Deze overweging lijkt des te billijker wanneer men er rekening mee houdt dat de werkgever de nodige inspanningen had gedaan om een inbreuk op de privacy van haar (niet verdachte) collega's uit te sluiten.

Toch kan men niet onverdeeld gelukkig zijn met dit standpunt, dat werkgevers een vrijgeleide geeft voor schending van de CAO (en mogelijk andere privacywetgeving) wanneer de daardoor vastgestelde inbreuk zwaarder zou wegen dan hun eigen overtreding. Dit standpunt moedigt werkgevers in zekere zin aan om te speculeren op de welwillendheid van een rechtbank ten aanzien van hun eigen inbreuken, wat de rechtszekerheid zeker niet ten goede komt.

2) Verplichte consultatie bij een dreigende inbreuk op de persoonlijke levenssfeer

De CAO heeft er rekening mee gehouden dat de camerabewaking een inbreuk kan vormen op de persoonlijke levenssfeer die voor de werknemers moeilijk aanvaardbaar zou kunnen zijn. Wanneer uit de verstrekte informatie blijkt dat de camerabewaking gevolgen kan hebben voor de persoonlijke levenssfeer van één of meerdere werknemers, dan schrijft artikel 10 een consultatiemechanisme voor.

In dit geval moet er een onderzoek worden georganiseerd naar de legitimiteit en de proportionaliteit van de maatregel, teneinde te verzekeren dat de inbreuk noodzakelijk is en tot een absoluut minimum wordt beperkt. In principe wordt het onderzoek op touw gezet door de ondernemingsraad of, bij ontstentenis daarvan, het comité voor preventie en bescherming op het werk.

Als de camerabewaking bovendien betrekking heeft op één van de doeleinden die enkel tijdelijke bewaking kunnen verantwoorden (namelijk de controle van de arbeid van de werknemer of van het functioneren van de werknemer in het productieproces) en/of er geen ondernemingsraad of een comité voor preventie en bescherming op het werk is, dan wordt het onderzoek uitgevoerd in samenspraak tussen de werkgever en de vakbondsafvaardiging.

Artikel 11 schrijft bovendien voor dat de ondernemingsraad of, bij ontstentenis daarvan, het comité voor preventie en bescherming op het werk bovendien regelmatig de gehanteerde bewakingssystemen moet evalueren en voorstellen doen met het oog op herziening in functie van de technologische ontwikkelingen. Op die manier kan een optimale bescherming van de persoonlijke levenssfeer worden verzekerd.

Fouilleren en doorzoeken van opslagruimtes

Fouilleren⁴² heeft een wettelijke basis gekregen via de Wet op het politieambt⁴³, maar het is duidelijk dat het toepassingsgebied van deze grondslag beperkt is tot dragers van de openbare macht, en dat werkgevers er zich dus op geen enkele manier kunnen beroepen.

Bij ontstentenis van een wettelijke grondslag lijkt een gedwongen fouilleringsactie louter door of op gezag van de werkgever dus uitgesloten, vermits moeilijk valt in te zien op welke manier er aan de vereisten van artikel 8 van het EVRM kan worden voldaan, zonder de daarin bepaalde criteria (legaliteit, legitimiteit en proportionaliteit) uit te rekken tot een punt waar ze alle betekenis verliezen.

Voor het doorzoeken van opslagkastjes wordt doorgaans echter meer begrip getoond. In een informele mededeling van de Privacycommissie⁴⁴ liet zij verstaan dat het principieel geoorloofd kan zijn om de kastjes van de werknemers te doorzoeken in geval van een vermoeden van diefstal. Hierbij moet wel rekening worden gehouden met het toepasselijke arbeidsreglement, de bestaande regelgeving en de normen die onder meer het EVRM vooropstelt.

Een legitieme zoeking van private opslagruimtes impliceert daarom dat de werknemer wordt verwittigd van de controle en het doel ervan⁴⁵. Wanneer mogelijk moet de toestemming van de werknemer worden gezocht. De controle mag bovendien niet disproportioneel zijn, moet de nodige discretie in acht nemen en bij voorkeur in de aanwezigheid van de werknemer worden uitgevoerd. In het concrete geval dat aanleiding gaf tot de verklaring van de Commissie gebeurde de controle conform het geldende arbeidsreglement, en in aanwezigheid van een vakbondsafgevaardigde.

Ten slotte vereist het principe van legitimiteit dat er voorafgaande ernstige aanwijzingen van misbruik zijn, zodat een systematische controle zonder enige duidelijke aanleiding (bijvoorbeeld een algemene verrassingscontrole zonder voorafgaand incident) te verregaand lijkt te zijn⁴⁶. De werknemer moet ten slotte ook de kans krijgen om zijn standpunt weer te geven over de resultaten van de controle.

Ook de rechtspraak heeft in het verleden dit standpunt onderschreven. Zo oordeelde het Arbeidshof van Brussel op 6 juni 1984⁴⁷ zelfs dat de volgehouden weigering van een werknemer om zijn opslagruimtes te laten doorzoeken door de werkgever een dringende reden voor ontslag kon uitmaken.

Een gelijkaardige houding kan worden aangenomen ten aanzien van het doorzoeken van een harde schijf of een gelijkaardig opslagmedium dat door de werkgever ter beschikking van de werknemer wordt gesteld⁴⁸. Net als bij de opslagkastjes gaat het om materiaal dat ter beschikking van de werknemer wordt gesteld als

⁴² Veelal omschreven als "het zintuiglijk speuren in, op of onder de kledij van een persoon teneinde er bepaalde stoffen, voorwerpen of sporen aan te treffen, zonder aanraking van intieme delen" (Cass. 27 oktober 1987, R.W. 1988-89, 1.025, noot P. ARNOU).

⁴³ Wet van 5 augustus 1992 op het politieambt, B.S. 22 december 1992

⁴⁴ Zie onder meer "Werkgever mag kastjes werknemers doorzoeken", De Metro, 28 september 2005, p.19

⁴⁵ Hoewel men in het licht van de hoger besproken Cassatierechtspraak hierrond vraagtekens kan plaatsen.

⁴⁶ Zie nochtans contra Arb.H. Brussel 6 juni 1982, Soc. Kron. 1984, dat oordeelde dat het volledig geoorloofd was om in het arbeidsreglement een regeling op te nemen die toeliet om op elk moment en zonder enige aanleiding kasten, gereedschapskoffers en dergelijke te onderzoeken, weliswaar in het bijzijn van de werknemer en enkel binnen de grenzen van de onderneming. De weigering om zich te onderwerpen aan een dergelijke controle werd zelfs aanvaard als dringende reden die een ontslag kon rechtvaardigen, tenminste indien de controle niet louter vexatoir was. Zie ook Arb.H. Gent 19 mei 1972, J.T.T. 1974, 26. De rechtspraak lijkt zich geleidelijk aan strenger op te stellen ten aanzien van dit soort regels.

⁴⁷ Arb.H. Brussel 6 juni 1984, Soc. Kron. 1984, 523.

⁴⁸ Zie over deze problematiek F.HENDRICKX, Elektronisch toezicht op het werk: Internet en camera's, Ced.Samsom, Diegem, 2000, p. 30 en volgende.

hulpmiddel voor de uitoefening van diens taken, maar dat desondanks integraal de eigendom blijft van de werkgever. Weliswaar kan de bestemming verschillen – zo zullen computers nagenoeg steeds een hoofdzakelijk professioneel doel dienen, terwijl de kastjes vaak specifiek bestemd zijn om persoonlijke goederen tijdelijk in op te slaan – maar de basisbeginselen van het controlerecht van de werkgever blijven gelijk.

Ook hier zal een controle dus veelal geoorloofd zijn, voor zover aan de voorwaarden van legaliteit, legitimiteit en proportionaliteit wordt voldaan. De redelijke houding van de werkgever en de aanwezigheid van een duidelijk arbeidsreglement spelen hierbij een doorslaggevende rol⁴⁹. Er moet wel opgemerkt worden dat computers ook vaak als communicatiemiddel worden gebruikt (bijvoorbeeld d.m.v. e-mail of instant messaging-software), zodat desgevallend de strengere regels van CAO 81 van toepassing kunnen zijn, evenals de andere bijzondere wetgeving die hieronder zal worden besproken.

Voor de controle van bestanden die niet verbonden zijn aan communicatiemiddelen (wat bijvoorbeeld het geval kan zijn voor tekstbestanden en spreadsheets) zijn echter enkel de algemene regels van het arbeidsrecht en de privacybescherming van toepassing, en niet de regels die verband houden met telecommunicatiebescherming.

Het beëindigen van de arbeidsrelatie

Als algemeen principe hoeft een ontslag naar Belgisch recht niet te worden gemotiveerd, zij het dat de gevolgen van het ontslag (met name de eventuele opzeggingsvergoeding) sterk kunnen wisselen naar gelang de ingeroepen grondslag. De privacy van de (ex-)werknemer kan vooral in het gedrang komen wanneer toepassing wordt gemaakt van artikel 32, 3° van de Arbeidsovereenkomstenwet, dat ontslag omwille van een dringende reden toestaat. In dit geval moet er namelijk wel een motivering worden voorzien, die eventueel een inbreuk op de persoonlijke levenssfeer kan vormen.

Het is namelijk mogelijk dat het ontslag wordt gebaseerd op een irrelevant persoonlijk gegeven, dat geen uitstaans heeft met de geschiktheid van de werknemer voor de betreffende functie. In feite is de situatie sterk gelijkaardig aan die van de sollicitatieprocedure: net zoals er tijdens de sollicitatie geen criteria mogen worden gebruikt die irrelevant zijn voor de functie (cf. supra), mogen deze criteria even min aan de basis liggen van het ontslag. Is dit toch het geval, dan is het ontslag foutief en kan het aanleiding geven tot schadeloosstelling van de ten onrechte ontslagen werknemer.

⁴⁹ F.HENDRICKX, Elektronisch toezicht op het werk: Internet en camera's, Ced.Samsom, Diegem, 2000, p. 26 en volgende.

Telecommunicatiemiddelen en toezicht

Probleemstelling

Telecommunicatiemiddelen vormen al jaren een essentieel werkmiddel voor de werknemers van de meeste bedrijven. Na de volledige inburgering van de telefonie zijn nu ook e-mail, surfen, SMS en instant messaging gangbare communicatiemechanismen geworden, en het ligt in de lijn van de verwachtingen dat deze lijst in de toekomst alleen nog maar zal groeien.

Dit impliceert ook dat deze communicatiemiddelen een enorme hoeveelheid gegevens bevatten die van fundamenteel belang zijn voor een onderneming. Informatie over bestellingen, contracten, conflicten, praktische afspraken, beleidsnormen enzovoorts worden steeds vaker elektronisch uitgewisseld. Vermits het vaak gegevens betreft die een grote potentiële impact kunnen hebben spreekt het voor zich dat de werkgever er een gerechtvaardigd belang bij heeft om deze informatiestroom voor zover mogelijk te controleren⁵⁰.

Niet alleen beschikt hij over een legitiem belang, ook de technische mogelijkheid tot een nagenoeg allesomvattende controle bestaat tegenwoordig. In een strak georganiseerd modern bedrijf kan alle elektronische communicatie immers digitaal via een centraal netwerk verlopen, waarbij alle mogelijke gegevens systematisch kunnen worden geregistreerd en voor een lange tijd opgeslagen. Daarbij is een zeker toezicht niet alleen nodig om gevoelige informatie te kunnen beheersen, maar ook om de goede werking van de infrastructuur te verzekeren.

Ook om zich in te dekken tegen moeilijke aansprakelijkheidsvragen kan een zekere controle dan ook geoorloofd zijn. Men kan zich bijvoorbeeld de vraag stellen of een onderneming niet een deel van de aansprakelijkheid draagt indien één van haar werknemers herhaaldelijk en systematisch afbeeldingen met een pornografische inslag verstuurt naar collega's – of a fortiori: cliënten – die hierom niet gevraagd hebben⁵¹.

Of nog: draagt een onderneming de eindverantwoordelijkheid indien haar netwerkbeheerder niet opmerkt dat een werknemer maandelijks gigabytes aan auteursrechtelijk beschermd materiaal downloadt of verdeelt via peer-to-peer netwerken? Het lijkt in dit soort gevallen duidelijk beter om te voorkomen via een toezichtsbeleid dan enkel te genezen via a posteriori reacties.

Ook hier stelt zich de vraag hoe ver de werkgever mag gaan. Het wordt immers veelal aanvaard dat werknemers in beperkte mate ook om persoonlijke redenen gebruik mogen maken van de communicatiemiddelen die hen ter beschikking worden gesteld. Mag de werkgever dan bijvoorbeeld alle e-mails van zijn werknemers nalezen, wel wetende dat een deel hiervan mogelijk voor persoonlijke redenen werd verstuurd en hij dus een inbreuk op hun privacy maakt? Onder welke voorwaarden en in welke mate mag hij de inhoud van hun communicatie analyseren? Op deze vraag gaan we in deze afdeling verder in.

⁵⁰ In dat verband kan bijvoorbeeld verwezen naar de bekende Amerikaanse Sarbanes-Oxley-wetgeving (in de wandelgangen als "SOX" aangeduid), die ondernemingen die op de Amerikaanse beurzen genoteerd zijn verplicht om alle uitgewisselde communicatie (inclusief informele of persoonlijke berichten) gedurende een bepaalde periode op te slaan. In België bestaat er geen equivalente regelgeving, temeer omdat dit op gespannen voet zou staan met onder meer het proportionaliteitsbeginsel van artikel 8 van het EVRM.

⁵¹ Wat onder meer strijdig zou kunnen zijn met het KB van 11 juli 2002 betreffende de bescherming tegen geweld, pesten en ongewenst seksueel gedrag op het werk (B.S. 7 november 1992).

Gebruik van telecommunicatiemiddelen door de werknemers

1) Controle op elektronische on-line communicatiegegevens: CAO 81⁵²

De belangrijkste juridische bron op dit vlak is CAO 81. Op een gelijkaardige manier als de hoger besproken CAO 68 heeft ook deze CAO als voornaamste oogmerk om uit te klaren op welke manier een toezichtsbeleid verzoend kan worden met de privacy van de werknemers, althans in de privésector. Hierbij werd rekening gehouden met de bepalingen van de Privacywet, evenals andere Belgische wetgeving die het telecommunicatiegeheim beschermt. In principe zou de CAO dus verzoenbaar moeten zijn met de bestaande wetgeving⁵³. In de afdelingen hieronder wordt nagegaan of dit klopt.

De CAO werd algemeen verbindend verklaard via een KB van 12 juni 2002⁵⁴. Zij regelt enkel de voorwaarden waaronder elektronische on-linecommunicatiegegevens mogen worden gecontroleerd. Elektronische on-linecommunicatiegegevens worden in de CAO met een wat verwarrende kringconstructie gedefinieerd als “de elektronische on-linecommunicatiegegevens s.l. ongeacht de drager via welke een en ander door een werknemer wordt overgebracht of ontvangen in het kader van de dienstbetrekking” (artikel 2 CAO).

Het is duidelijk de bedoeling om een brede interpretatie aan deze term te geven, die volgens de commentaren bij de CAO “ruim genoeg is om alle on-linetechnologieën te omvatten, rekening houdend met de toenemende verwevenheid en de snelle ontwikkeling van deze technologieën en de drager die wordt gebruikt. [De CAO] is dan ook van toepassing ongeacht deze drager. Zij viseert bovendien de elektronische on-linecommunicatie, zowel intern als extern.”

De CAO is dus niet van toepassing op andere communicatiemiddelen (zoals briefwisseling via de klassieke post of traditionele telefonie⁵⁵), noch regelt zij de toegang tot en/of het gebruik van de elektronische on-linecommunicatiemiddelen. Ze regelt enkel de voorwaarden waaronder de werkgever elektronische on-linecommunicatiegegevens op de werkplek mag verzamelen met het oogmerk om ze te controleren en te verwerken zodat ze aan een werknemer kunnen worden toegeschreven.

De CAO sluit dus niet uit dat de werkgever het gebruik van bepaalde toepassingen (zoals peer-to-peer-netwerken) zou verbieden of beperken (bijvoorbeeld door websites enkel toegankelijk te maken indien ze voorkomen op een vooraf gecontroleerde “white list”), of dat hij bepaalde communicatiemiddelen of –media (bijvoorbeeld het Internet) integraal uitsluit. De bepaling van de gepaste werkmiddelen van de werknemers is immers een prerogatief van de werkgever⁵⁶.

⁵² Voor een uitgebreide bespreking van deze CAO kan ook worden verwezen naar R.BLANPAIN en M.VANGESTEL, Gebruik en controle van e-mail, intranet en Internet in de onderneming – Praktijk en recht, Die Keure, Brugge, 2003, p. 144 en volgende.

⁵³ CAO's mogen immers niet ingaan tegen bepalingen van dwingend recht (artikel 51 van de wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités), en dit ongeacht of ze al dan niet algemeen verbindend werden verklaard. Met andere woorden: de CAO mag niet in strijd zijn met de Afluisterwet en de Wet inzake Elektronische Communicatie (hieronder besproken).

⁵⁴ KB van 12 juni 2002 waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst nr. 81 van 26 april 2002, gesloten in de Nationale Arbeidsraad, tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatie-gegevens, B.S. 5 oktober 2002.

⁵⁵ In tegenstelling dus tot VoIP-telefonie, waarbij de geluidsignalen worden omgezet naar digitale pakketjes die middels het standaard-TCP/IP-protocol via het Internet worden verplaatst. Deze technologie lijkt wel onder CAO 81 te vallen.

⁵⁶ Cf. artikel 2, 3 en 20 van de Arbeidsovereenkomstenwet.

Dit impliceert ook - qui peut le plus, peut le moins – dat hij grenzen mag opleggen aan het private gebruik van de telecommunicatiemiddelen, die via de arbeidsovereenkomst of het arbeidsreglement kenbaar kunnen worden gemaakt. De werkgever kan hierbij zeer ver gaan, hoewel de volledig uitsluiting van privégebruik steeds minder wordt aanvaard^{57,58}. Bij ontstentenis van expliciete bepalingen hierover wordt aanvaard dat een beperkt redelijk privégebruik – in de praktijk in concreto te appreciëren – toelaatbaar is. Om misverstanden hierover te vermijden is het desondanks aan te raden om de grenzen van toelaatbaar privégebruik expliciet kenbaar te maken aan de werknemers middels een communicatietoezichtsbeleid.

Het uitgangspunt van de CAO is een wederzijdse erkenning van de belangen van de werknemers en de werkgevers. Artikel 3 stelt dat:

- de werknemers erkennen het beginsel volgens hetwelk de werkgever het recht heeft controle uit te oefenen op het werkinstrument en op het gebruik dat de werknemer ervan maakt in het kader van de uitvoering van zijn contractuele verplichtingen, ook wanneer dit gebruik binnen de persoonlijke levenssfeer valt, rekening houdend met de in deze overeenkomst bepaalde toepassingsregels;
- de werkgevers eerbiedigen het recht van de werknemers op bescherming van hun persoonlijke levenssfeer in het kader van de dienstbetrekking en de rechten en verplichtingen die er voor iedere partij uit voortvloeien.

Deze wederzijdse erkenning is belangrijk als uitgangspunt. Het wordt immers nauwelijks betwist dat de werknemers een zeker recht hebben op de bescherming van hun privacy bij het gebruik van telecommunicatiemiddelen, zelfs in het kader van een arbeidsbetrekking. Omgekeerd wordt wel nog beweerd dat dit principiële recht op privacy elke algemene en permanente controle van de werkgevers in de communicatie van de werknemers uitsluit. Elke inmenging zou dan de voorafgaande instemming van de betrokken werknemer vereisen, of minstens duidelijke aanwijzingen van misbruik. De CAO opteerde dus voor een meer genuanceerd en praktisch standpunt.

Bij de implementatie van een communicatietoezichtsbeleid met betrekking tot elektronische on-linecommunicatiegegevens zal de werkgever zich evident moeten houden aan de bepalingen van de Privacywet. De grondbeginselen van deze wet, waaronder finaliteit, proportionaliteit en transparantie, spelen dan ook een fundamentele rol in de context van de CAO. Hiermee wordt zowel rekening gehouden bij het bepalen van de toelaatbaarheid van een bepaald beleid als bij de procedure die moet worden gevolgd om de geregistreerde gegevens toe te mogen schrijven aan een bepaalde werknemer.

⁵⁷ Zie in die zin artikel 11 van CAO 81, met betrekking tot de individualisering van communicatiegegevens: "De tenuitvoerlegging ervan mag niet leiden tot de ondoelmatigheid van de waarborgen die deze collectieve arbeidsovereenkomst aan de werkgevers en de werknemers biedt door het verlenen van een uitsluitend beroepsmatig of privé-karakter aan het geheel van elektronische on-linecommunicatiegegevens." (eigen cursivering). Tevens: F.HENDRICKX, Elektronisch toezicht op het werk: Internet en camera's, Ced.Samsom, Diegem, 2000, p. 36 en volgende.

⁵⁸ Contra: R.BLANPAIN en M.VANGESTEL, Gebruik en controle van e-mail, intranet en Internet in de onderneming – Praktijk en recht, Die Keure, Brugge, 2003, p. 168, waar de auteurs het standpunt onderschrijven dat werkgevers privégebruik wel degelijk integraal mogen uitsluiten. Zie voor een toepassing van dit laatste standpunt in de praktijk Arbh. Luik, 17 mei 1985, J.T.T. 1985, 472; of nog Arbh. Antwerpen, 8 januari 2003, Soc. Kron. 2003, 193.

2) Controle op de elektronische on-linecommunicatiegegevens

De instelling van een controlemechanisme op elektronische on-linecommunicatiegegevens is slechts toegestaan onder een beperkt aantal voorwaarden.

Op de eerste plaats moet de controle een legitiem doeleinde hebben. Volgens artikel 5 van de CAO kunnen er maar 4 doeleinden hieraan voldoen. De controle mag enkel de volgende doelstellingen nastreven (artikel 5 CAO 81):

- 1° het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- 2° de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken;
- 3° de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming;
- 4° het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van on-linetechnologieën.

Het gaat om vrij brede bepalingen die in nagenoeg elke onderneming van toepassing kunnen zijn. Zo heeft elke onderneming er wel belang bij om bijvoorbeeld op te treden tegen racistische misdrijven via zijn netwerk (§1, 1°), of om dataverkeer te registreren om de netwerkbelasting te kunnen nagaan (§1, 3°).

De echte beperking van artikel 5 bevindt zich dan ook in §2: om geoorloofd te zijn moet de werkgever duidelijk en expliciet de doelstelling(en) van de controle omschrijven. Het finaliteitsvereiste komt daardoor in de praktijk eerder neer op een informatieverplichting: de werkgever zal zijn werknemers – bijvoorbeeld via het arbeidsreglement of een policydocument – moeten inlichten van het gevoerde observatiebeleid. Bij ontbreken van deze mededeling loopt men het risico strafrechtelijk bestraft te worden wegens een inbreuk op het telecommunicatiegeheim, zoals hieronder zal worden besproken.

Een voorbeeld van de nefaste gevolgen van het gebrek aan een privacybeleid vindt men in de zaak K.⁵⁹. In deze zaak moest het Arbeidshof van Brussel zich uitspreken over het vermeend onrechtmatig ontslag van mijnheer K., die in een informaticabedrijf was tewerkgesteld onder de leiding van de heer D.V.. Enkele maanden nadat D.V. het bedrijf verliet contacteerde hij K. per e-mail met het verzoek om hem vertrouwelijke loongegevens door te sturen. K. gaf hieraan gevolg.

De vennootschap had een niet-concurrentiebeding opgenomen in haar overeenkomst met D.V., maar vreesde – kennelijk terecht – dat hij dit beding niet zou naleven. Om die reden filterde zij het e-mailverkeer,

⁵⁹ Arb.H. Brussel 15 december 2004, Computerr. 2005, 47, met noot P.MAERTEN. Zie ook DUMORTIER, J., "ICT & privacy op de werkvloer. De zaak K.", Trends Business ICT, juni 2005

op zoek naar mogelijk ongeoorloofd contact tussen D.V. en haar werknemers. De e-mail tussen K. en D.V. werd onderschept, waarna K. werd ontslagen wegens dringende reden.

K. ging hiermee echter niet akkoord en wendde zich tot de Arbeidsrechtbank, die hem in het ongelijk stelde. Het Arbeidshof volgde echter wel de redenering van K.: door de inhoud van alle e-mails systematisch te controleren zonder de werknemers hiervan op de hoogte te brengen schond de vennootschap de privacywetgeving. Het aangebrachte bewijsmateriaal werd daarom als onwettig aangemerkt, en de vennootschap werd veroordeeld tot betaling van een ontslagvergoeding van 23.000 Euro en de kosten van het geding. In het licht van de hierboven geciteerde Cassatierechtspraak⁶⁰ kan men vraagtekens plaatsen bij deze beslissing. Minstens lijkt de rechtspraak momenteel weinig voorspelbaar te zijn.

Daarnaast mag de geplande controle niet disproportioneel zijn⁶¹. Dit impliceert met name dat het toezicht geen grotere inbreuk op de persoonlijke levenssfeer van de werknemers met zich mag meebrengen dan strikt noodzakelijk is voor de verwezenlijking van de meegedeelde doeleinden van de controle (artikel 6).

Indien men bijvoorbeeld enkel het totale volume van de verzonden e-mails wil controleren, dan is het niet noodzakelijk om de inhoud van deze mails na te gaan, en zelfs niet om te bepalen wie de verzender of de ontvanger was (hoewel dit om andere redenen wel interessant en geoorloofd kan zijn). Op dezelfde manier kan men controleren hoe vaak en hoe lang een bepaalde website door de werknemers wordt bezocht, zonder noodzakelijkerwijs te moeten nagaan wie er precies tijd doorbrengt op de site. Wenst men daarentegen wel het gedrag van individuele werknemers na te gaan, dan moet men rekening houden met de bepalingen in verband met de individualisering van gegevens die hieronder worden besproken.

Ten slotte worden er in de artikelen 7 en volgende bepaalde transparantievereisten vooropgesteld, die de werknemer moeten toelaten op de hoogte te blijven van het toezichtsbeleid van zijn werkgever, en die hem zelfs een zekere inspraak hierin verlenen. Het mechanisme is in feite zeer gelijkaardig aan dat van CAO 68. Dit is ook niet vreemd, vermits beide CAO's in verregaande mate een verbijzondering zijn van de Privacywet met betrekking tot toezicht in een arbeidscontext.

Ook hier is de geprivilegieerde gesprekspartner bij de invoering van een controlesysteem de ondernemingsraad. Deze moet voordat het toezicht wordt ingesteld op de hoogte worden gebracht van de doeleinden, de vraag of persoonsgegevens al dan niet bewaard zullen worden en de manier waarop, het al dan niet permanente karakter van de controle⁶², en de details aangaande het controlebeleid, inclusief de prerogatieven van de werkgever en het toezichthoudend personeel.

Beschikt de onderneming niet over een ondernemingsraad, dan wordt het comité voor preventie en bescherming op het werk geïnformeerd of, bij ontstentenis daarvan, de vakbondsafvaardiging of ten slotte bij ontstentenis daarvan: de werknemers zelf. Ook hier wordt er dus getracht de informatie te richten op het meest invloedrijke professionele orgaan binnen de onderneming.

⁶⁰ Het Hof van Cassatie besliste onlangs om videobeelden die verkregen waren met miskenning van de informatieplicht van de werkgever desondanks toe te laten als bewijsmateriaal. Cass. 2 maart 2005, n. gepubl., on-line beschikbaar via www.juridat.be; cf. supra.

⁶¹ Zie hierover ook Advies nr. 10/2000 van 3 april 2000 van de Privacycommissie: "Iedere controle zou gericht moeten zijn en gerechtvaardigd door aanwijzingen die doen vermoeden dat er misbruik wordt gemaakt van de werkinstrumenten. Een algemene controle a priori op alle telecommunicatiegegevens, evenals de systematische registratie van al deze gegevens, lijkt disproportioneel ten opzichte van het nagestreefde doel."

⁶² In tegenstelling tot bij CAO 68 is de toelaatbaarheid van een permanente controle dus niet beperkt tot toezicht voor bepaalde doelstellingen.

Net als in CAO 68 is de werkgever steeds verplicht om dezelfde informatie ook rechtstreeks te verstrekken aan de betrokken werknemers op het moment van de installatie van het controlesysteem⁶³. Daarnaast moet de werknemer ook worden geïnformeerd over de communicatie-instrumenten waarover hij mag beschikken, het toegelaten en verboden gebruik ervan en de toepasselijke sancties wanneer deze regels worden genegeerd. Volgens artikel 8 mag de werkgever vrij het gekozen informatiemedium kiezen, maar moet de informatie wel steeds effectief, begrijpelijk en bijgewerkt zijn. De informatie kan bijvoorbeeld via circulaire of gedragscodes worden verspreid, maar kan ook gewoon een deel uitmaken van het algemene arbeidsreglement of de arbeidsovereenkomst.

Artikel 10 schrijft bovendien voor dat de geïnstalleerde controlesystemen regelmatig moeten worden geëvalueerd, naar gelang het geval in de ondernemingsraad, het comité voor preventie en bescherming op het werk of met de vakbondsafvaardiging, met het oog op voorstellen om ze aan te passen aan de technologische ontwikkelingen. Op die manier moet worden verzekerd dat de inbreuk op de persoonlijke levenssfeer nooit verder reikt dan strikt noodzakelijk is.

3) Individualisering van elektronische on-linecommunicatiegegevens

Zoals al eerder vermeld zijn de procedures en de voorwaarden die hierboven worden beschreven enkel afdoende wanneer de werkgever elektronische on-linecommunicatiegegevens controleert zonder deze te individualiseren, m.a.w. zonder de oorsprong van de gegevens toe te schrijven aan een specifiek geïdentificeerde of identificeerbare bron (artikel 12 CAO 81). Wanneer de werkgever de verzamelde gegevens echter wel aan een specifieke persoon wil toeschrijven moet er aan extra voorwaarden worden voldaan.

De CAO heeft in de eerste plaats betrekking op de individualisering van de elektronische communicatiegegevens, wat niet noodzakelijk impliceert dat er ook kennis mag worden genomen van de inhoud ervan. De CAO maakt hierbij een rigide onderscheid tussen communicatie waarvan het louter beroepsmatige karakter niet wordt betwist, en communicatie die een persoonlijke inhoud zou kunnen hebben. “Wanneer het onderwerp en de inhoud van de elektronische on-linecommunicatiegegevens een beroepsmatig karakter hebben dat door de werknemer niet in twijfel wordt getrokken, zal de werkgever zonder enige procedure kennis kunnen nemen van deze gegevens.”, aldus het verslag bij de CAO.

Wanneer het privé-karakter van de inhoud van deze gegevens daarentegen blijkt uit bijvoorbeeld bepaalde informatie in het onderwerp van een e-mailbericht, dan moet de individualiseringsprocedure worden gebruikt. Hoe dan ook mag er van de inhoud van de berichten slechts uitzonderlijk kennis worden genomen⁶⁴. Met name moet er rekening worden gehouden met de invloed van de wetgeving die hieronder nog zal worden besproken, zoals de Privacywet en alle andere regelgeving die het telecommunicatiegeheim beschermt.

⁶³ Hoewel ook hier verwezen kan worden naar het hierboven aangehaalde Cassatie-arrest van 2 maart 2005 dat schending van deze verplichting in bepaalde situaties geoorloofd vindt; of beter: dat een dergelijke schending geen grond is voor het weren van onrechtmatig verkregen bewijsmateriaal uit een procedure.

⁶⁴ Een vaak geciteerde toepassing hiervan is het Nikon-arrest van het Franse Hof van Cassatie, waarin werd geoordeeld dat kennisname van de inhoud van een persoonlijk bericht dat tijdens de arbeidsduur door een werknemer werd verzonden via de infrastructuur van zijn werkgever een onrechtmatige inbreuk kon uitmaken op de persoonlijke levenssfeer van de werknemer, zelfs indien de werkgever expliciet het privégebruik van de infrastructuur had verboden. Cass.Fr. 2 oktober 2001, J.T.T. 2002, 37.

De inhoud van elektronische on-linecommunicatie is met andere woorden in zeer verregaande mate beschermd wanneer het louter beroepsmatige karakter⁶⁵ ervan niet vaststaat⁶⁶.

De vraag dringt zich op in welke mate de regelgeving op dit vlak voldoende is aangepast aan de realiteit. Overmatig gebruik van het e-mailsysteem voor persoonlijke communicatie kan bijvoorbeeld moeilijk aantoonbaar zijn zonder kennisname van de inhoud.

Zo zag de Arbeidsrechtbank van Brussel zich in mei 2000 geconfronteerd met een arbeidsgeschil waarbij de werknemer werd ontslagen wegens overmatig privégebruik van de e-mailfaciliteiten van het bedrijf⁶⁷.

De werkgever koesterde voor het eerst verdenkingen toen de werknemer, een informaticaverantwoordelijke, er niet in slaagde om zijn opdrachten tijdig af te werken en deadline na deadline miste. Daarop besloot de werkgever zijn e-mails van de voorbije paar maanden stuk voor stuk na te lezen. Deze controle bracht aan het licht dat de informaticus een wel zeer vriendschappelijke e-mailrelatie onderhield met één van zijn collega's.

De werknemer werd ontslagen wegens dringende reden, vermits duidelijk bleek dat hij frequent uren tijd verspeelde aan het verzenden van privéberichten. Daarop volgde een rechtszaak: de ex-werknemer beweerde dat de controle onrechtmatig en buitensporig was, en dat zijn gedrag bovendien niet laakbaar was gezien de kwetsbare emotionele positie van zijn collega op dat moment. De werkgever stelde een tegeneis in als compensatie voor de verloren arbeidsuren.

De arbeidsrechtbank besloot uiteindelijk om beide partijen gedeeltelijk in het gelijk te stellen. Volgens haar maakte het gedrag van de ex-werknemer een gewoonlijk voorkomende lichte fout uit, en betrof het dus een onrechtmatigheid die aanleiding moest geven tot een schadevergoeding. De werkgever was echter eveneens te ver gegaan: het gedrag van de werknemer zou niet zwaarwichtig genoeg zijn om als dringende reden te volstaan. Daarbij was de kennisname van de inhoud van de berichten volgens de rechtbank buitensporig. De rechtbank hield ook en vooral rekening met het lakse gedrag van de werkgever, die voorafgaand aan de kennisname van de e-mails op geen enkele manier controle had uitgeoefend op de ondermaatse prestaties van de werknemer.

Ook het al dan niet zorgvuldige gedrag van de werkgever voorafgaand aan de controle is dus een factor waarmee rekening kan worden gehouden bij de beoordeling van de legitimiteit en de proportionaliteit van een controlemaatregel. Dit is in het bijzonder het geval wanneer de resultaten van de maatregel worden ingeroepen als een dringende reden voor ontslag. Het eindresultaat is dus zeer gelijkaardig aan de hierboven besproken zaak K.: ook hier werd de werkgever veroordeeld omdat hij verzuumde te voldoen aan zijn verplichtingen die voortvloeien uit de vigerende privacywetgeving.

⁶⁵ Men kan bijvoorbeeld denken aan het telefonisch of via e-mail verzenden van beursorders, waar de automatische en integrale registratie van de inhoud van de berichten niet als disproportioneel zal worden aangemerkt, vermits de bewijswaarde van deze opnames een voorwaarde is voor een acceptabel risicobeheer in een beursonderneming. Deze situatie werd ook specifiek behandeld in artikel 128 van de hieronder besproken Wet Elektronische Communicatie, dat registratie van dergelijke telecommunicatie toelaat wanneer de betrokken partijen hierover vooraf worden geïnformeerd.

⁶⁶ Zie hierover ook Advies nr. 10/2000 van 3 april 2000 van de Privacycommissie: "Wat de elektronische post betreft, is de Commissie van oordeel dat de kennisneming van de inhoud van de e-mails overmatig is, en indruist tegen de hierboven vermelde wettelijke bepalingen, net zoals het af luisteren of opnemen van de telefoongesprekken van de werknemer dat zouden zijn."

⁶⁷ Arb.Rb. Brussel 2 mei 2000, Computerr., 2001, p.26, noot D.CASAER.

Het finaliteits- en proportionaliteitsbeginsel worden verder uitgewerkt via artikel 13 en 14 van de CAO. In feite voegen deze artikelen weinig nieuws toe: de verzamelde gegevens mogen enkel worden verwerkt indien dit te goeder trouw gebeurt, verzoenbaar is met de doeleinden die de werkgever heeft aangegeven en als alle maatregelen worden genomen om interpretatiefouten te vermijden. Evident moeten de verwerkte gegevens toereikend, ter zake dienend en niet overmatig zijn, overeenkomstig de bepalingen van de Privacywet. Wat betreft de te volgen procedure is de CAO wat specifiek.

De CAO maakt hier het onderscheid tussen individualisering via een directe en via een indirecte procedure, afhankelijk van de oorspronkelijk aangekondigde doeleinden van de controle. In het eerste geval mag de werknemer rechtstreeks worden geïdentificeerd; in het tweede geval moet er een voorafgaande voorlichtingsfase worden voltooid.

De directe individualisering is toegelaten wanneer de controle één of meerdere van de eerste drie hoger vermelde doelstellingen viseert (artikel 5, §1, 1°-3°; namelijk het voorkomen van ongeoorloofde of lasterlijke feiten; de bescherming van de economische, handels- en financiële belangen van de onderneming; en het waarborgen van de veiligheid en/of de goede technische werking van de IT-netwerksystemen). In deze gevallen wordt het belang van de onderneming als dusdanig zwaarwichtig beschouwd dat de individualisering geen verdere kennisgeving aan de betrokkene vereist.

Wanneer de controle daarentegen bestemd was om de naleving te goeder trouw van de beginselen en regels voor het gebruik van on-linetechnologieën na te gaan (artikel 5, §1, 4°), dan verplicht de CAO de werkgever om een bijkomende voorlichtingsfase te volgen alvorens de individualisering is toegelaten. Het gaat in deze hypothese veelal om gedragingen die als ongewenst worden beschouwd omdat ze de productiviteit van de onderneming ongunstig beïnvloeden of sociaal ongewenst zijn, maar die als dusdanig niet illegaal zijn of een ernstige dreiging vormen voor de belangen van de onderneming of de goede werking van de infrastructuur. Een typevoorbeeld is het bekijken van (legaal) pornografisch materiaal tijdens de werkuren, of het overmatig versturen van grappig bedoelde e-mails.

In dit geval erkent de CAO dat optreden dus ook mogelijk moet zijn, maar dat er een enigszins subtielere aanpak moet worden gevolgd. Artikel 16, §2 geeft aan dat de werknemer tijdens de voorlichtingsfase eerst moet worden ingelicht over het bestaan van de onregelmatigheid (m.a.w. hij moet er op worden gewezen dat zijn gedrag in strijd is met de geldende regels), en dat bij verdere onregelmatigheden zijn gegevens zullen worden geïndividualiseerd. De bedoeling is dus dat de werknemer erop wordt gewezen dat zijn gedrag onaanvaardbaar is, en dat verdere inbreuken in sancties kunnen resulteren. Het gaat om een waarschuwingsprocedure die in de praktijk best op een geautomatiseerde manier wordt ingericht, vermits een persoonlijke behandeling veelal voorafgaande individualisering impliceert.

Sorteert de waarschuwing niet het gewenste resultaat en begaat de werknemer een nieuwe overtreding, dan wordt hij met toepassing van artikel 17 van de CAO door de werkgever uitgenodigd voor een persoonlijk gesprek, waarbij zijn gegevens dus noodzakelijkerwijs worden geïndividualiseerd. Dit gesprek moet worden gevoerd alvorens er enige beslissing over het lot van de werknemer wordt genomen.

Het volstaat dus zeker niet dat het "gesprek" bestaat uit een loutere kennisgeving van een tuchtmaatregel of a fortiori een ontslag om dringende redenen. Het is daarentegen de bedoeling om een dialoog tot stand te brengen met de werknemer over zijn herhaalde laakbare gedrag, zodat hij zijn standpunt uiteen kan

zetten alvorens een eventuele sanctie wordt opgelegd. Artikel 17, §2 expliciteert echter dat een schorsingsmaatregel niet onder deze regeling valt, zodat de arbeidsovereenkomst wel kan worden geschorst zonder de werknemer voorafgaandelijk te horen.

Naast deze CAO moet er natuurlijk nog met de andere toepasselijke rechtsnormen rekening worden gehouden. Hieronder gaan we op de belangrijkste Belgische regelgeving in.

1) Verwerking van persoonsgegevens

De registratie van telecommunicatiegegevens zal vaak ook een verwerking van persoonsgegevens zijn die onder het toepassingsgebied van de Privacywet valt. Dit is niet het geval wanneer de geregistreerde gegevens niet aan een individu kunnen worden toegeschreven (bijvoorbeeld bij de automatische aanmaak van anonieme statistieken over bezochte sites, e-mailvolume of gemiddelde telefoonduur). Wanneer de gegevens echter wel kunnen worden herleid tot een individu (zoals bij de registratie van een IP-adres, afzendadres of telefoonnummer) dan is de Privacywet integraal van toepassing.

Vermits CAO 81 bedoeld is als verduidelijking van de verplichtingen van de Privacywet die specifiek zijn voor de verwerking van telecommunicatiegegevens wordt er hier niet opnieuw op de details ingegaan.

2) De Wet Elektronische Communicatie en de Afluisterwet

De bescherming van de persoonlijke levenssfeer van de werknemer die gebruik maakt van telecommunicatiemiddelen wordt niet enkel beschermd door het arbeidsrecht, de Privacywet en de nodige CAO's. Het telecommunicatiegeheim wordt – net als het briefgeheim – ook strafrechtelijk beschermd. De voornaamste juridische bronnen hiervoor zijn de zogenaamde Afluisterwet⁶⁸ en de Wet Elektronische Communicatie (WEC)⁶⁹. Beide wetten bekijken hetzelfde probleem vanuit een ander standpunt.

De Afluisterwet voegde onder meer de artikelen 259bis en 314bis⁷⁰ toe aan het strafwetboek. Deze artikelen bestraffen op de eerste plaats de opzettelijke kennisname of opname van de inhoud van privé-telecommunicatie⁷¹ tijdens de overbrenging⁷² ervan met behulp van een toestel door eender wie er niet aan deelneemt. Een dergelijke kennisname is enkel toegelaten mits toestemming van alle deelnemers aan die telecommunicatie.

⁶⁸ Wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en openen van privé-communicatie en -telecommunicatie, B.S. 24 januari 1995

⁶⁹ Wet van 13 juni 2005 betreffende de elektronische communicatie, B.S. 20 juni 2005.

⁷⁰ De artikelen zijn nagenoeg identiek. Het voornaamste verschil is de hoedanigheid van de dader: artikel 259bis Sw. is van toepassing op dragers van de openbare macht voor gedragingen tijdens de uitoefening van hun functie; artikel 314bis is van toepassing op particulieren. Voor dit hoofdstuk is dus in feite enkel artikel 314bis relevant.

⁷¹ Het begrip "privé-telecommunicatie" is erg ruim. "Privé" moet hier worden begrepen als "niet bestemd om door iedereen te worden ontvangen", en sluit arbeidssituaties dus niet uit.

⁷² Dit is een moeilijk te interpreteren voorwaarde, die in de praktijk steeds moet worden geëvalueerd. Zo kan bij e-mail worden geargumenteerd dat deze artikelen niet meer van toepassing zijn wanneer de e-mail wordt geraadpleegd na de aankomst ervan in de mailbox van de gebruiker. Men zou echter net zo goed het standpunt kunnen innemen dat de overbrenging slechts is voltooid na effectieve kennisname van de ontvangst van het bericht. Wellicht zal dit criterium nog in de praktijk moeten worden geapprecieerd door de rechtspraak.

Gelijkaardige straffen worden voorzien voor het opstellen van af luisterapparatuur met het opzet dit misdrijf te plegen, of het gebruiken, bewaren of verspreiden van onwettig opgenomen berichten.

De WEC bekijkt ditzelfde probleem in artikel 124⁷³ vanuit een andere invalshoek. Zonder toestemming van alle betrokken partijen verbiedt dit artikel de opzettelijke kennisname van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor de onderschepper is bestemd, evenals van gegevens inzake elektronische communicatie met betrekking tot een andere persoon. De opzettelijke identificatie van de betrokkenen wordt ook verboden, evenals het gebruiken, bewaren of verspreiden van de onderschepte informatie.

Kort samenvattend kan worden gezegd dat de Afluisterwet kennisname van de inhoud van een privébericht verbiedt, terwijl de WEC kennisname van het bestaan hiervan verbiedt. Het eerste impliceert vanzelfsprekend het tweede; maar niet noodzakelijk omgekeerd. Wie bijvoorbeeld opzettelijk gegevens onderschept die aantonen dat een bepaald persoon op een gegeven moment een e-mail heeft verstuurd naar een correspondent kan daardoor de WEC overtreden, zonder noodzakelijkerwijs de Afluisterwet te schenden. Immers, het is denkbaar dat de inhoud van de e-mail hierbij verborgen blijft.

In een arbeidsrechtelijke context zouden deze bepalingen ver reikende gevolgen kunnen hebben. Immers, een werkgever zal bij de registratie van de telecommunicatie van zijn werknemers nagenoeg steeds de Afluisterwet en/of de WEC schenden, tenzij hij zich op een uitzondering kan beroepen. Hierbij heeft de rechtspraak in het verleden al expliciet bevestigd dat de band van juridische ondergeschiktheid die voortvloeit uit de Arbeidsovereenkomstenwet in se niet voldoende is om een inbreuk op het telecommunicatiegeheim te verantwoorden⁷⁴. Ook de toestemming van de werknemer is maar een gedeeltelijke oplossing. Immers, om bijvoorbeeld de e-mail te lezen van een werknemer is niet alleen zijn toestemming nodig, maar ook die van alle betrokken correspondenten.

Dit zou tot de onhoudbare oplossing leiden dat de werkgever de toestemming zou moeten vragen aan zijn cliënteel om kennis te mogen nemen van de berichten die zij naar zijn werknemers hebben gestuurd. Een beroep op CAO 81 als afwijkende "lex specialis" biedt hierbij geen soelaas: als strafrechtelijke bepalingen hebben de relevante artikels van de Afluisterwet en de WEC een dwingend karakter. Bijgevolg kan ervan niet worden afgeweken bij CAO⁷⁵, zodat de bepalingen van CAO 81 in geval van strijdigheid met de Afluisterwet en de WEC geen toepassing kunnen vinden.

De WEC en de Afluisterwet verbieden echter enkel kennisname van telecommunicatie door derden. Er kan worden geargumenteed dat de werkgever geen derde is⁷⁶: hij is immers veelal de eigenaar van de gebruikte infrastructuur, heeft een toezichtsrecht dat zelfs een steunpilaar is van zijn verhouding met zijn werknemers, en bovenal moet hij aanvaarden dat zijn werknemers hem vertegenwoordigen ten aanzien van zijn cliënten,

⁷³ Voorheen: artikel 109terD van de Wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (de zogenaamde Belgacomwet), B.S., 27 maart 1991

⁷⁴ Zie Arb.H. Brussel 15 december 2004, Computerr. 2005, 47, met noot PMAERTEN: "Dat art.17, 2° WAO de werkgever op grond van zijn patronaal gezag een vrijbrief zou geven om registratie toe te laten in de zin van artikel 109terE van de wet kan niet worden aanvaard. De bepaling is te weinig precies om een beperking van een grondrecht te kunnen verantwoorden."

⁷⁵ Artikel 51 van de wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités, B.S. 15 januari 1969

⁷⁶ Zie in die zin R.BLANPAIN en M.VANGESTEL, Gebruik en controle van e-mail, intranet en Internet in de onderneming – Praktijk en recht, Die Keure, Brugge, 2003, p. 153.

indien niet in rechte, dan toch minstens in feite. Men kan daarom in vraag stellen of de werkgever wel een “derde” is in de zin van deze wetten.

Ons inziens kan men niet concluderen dat deze gezagsverhouding een kwalificatie als derde uitsluit. Het oogmerk van deze wetten is immers de bescherming van het telecommunicatiegeheim, dat een essentieel aspect is van de persoonlijke levenssfeer. Welnu, indien men erkent dat professionele activiteiten van de werknemer niet verstoken mogen blijven van persoonlijke contacten – zoals het overbekende arrest Niemitz⁷⁷ oordeelde – dan kan men niet oordelen dat een werkgever zich niet aan de beperkingen van de toepasselijke privacywetgeving hoeft te houden.

Indien men dit a contrario wel zou doen, door te oordelen dat de werkgever geen derde is en dus geen toestemming van de betrokken partijen behoeft, dan miskent men voor een groot deel de uitwerking van het arrest Niemitz. Dit arrest erkent immers dat het recht van de werknemers op respect voor hun persoonlijke levenssfeer niet eindigt wanneer zij de werkvloer betreden. Daarbij zou deze interpretatie ook voorbijgaan aan de vaststelling dat de werkgever hoe dan ook een derde is vanuit het standpunt van de communicatiepartner van de werknemer, die immers niet (noodzakelijk) in een gezagsverhouding tot de werkgever staat.

De toepasselijkheid van deze artikelen is overigens niet onverzoenbaar met het normale functioneren van de goede onderneming. Immers, werknemers geven hun toestemming tot een beperkte controle door het aangaan van een arbeidsrelatie, terwijl van derden verondersteld kan worden dat hun professionele communicatie de stilzwijgende toestemming bevat om kennis te nemen van hun communicatiegegevens voor zover dit nodig is voor de correcte behartiging van hun zakelijke belangen. Door in de uitgewisselde e-mails te verwijzen naar een disclaimer waarin wordt aangegeven dat de mails worden vermoed een professioneel karakter te hebben kan dit probleem verder worden opgelost⁷⁸. Noch de WEC, noch de Afluisterwet vereisen immers een expliciete toestemming: een stilzwijgende toestemming kan volstaan wanneer deze ondubbelzinnig is⁷⁹. Deze toestemming kan dus worden afgeleid uit het gedrag van de derde.

Ons inziens moet aldus niet besloten worden dat de Afluisterwet en de WEC niet van toepassing zijn in een arbeidsrelatie, maar enkel dat in deze specifieke context rekening moet worden gehouden met de (eventueel impliciet) uitgedrukte wens van de betrokken partijen (enerzijds de werknemer, anderzijds de cliënt). De nuance is niet zonder belang.

Weliswaar leidt de principiële toepasbaarheid van deze beide wetten in een arbeidscontext tot een bepaalde rechtsonzekerheid, vermits men steeds zal moeten afwegen of een bepaalde kennisname verzoenbaar is met de verwachtingen van de betrokken partij. Maar anderzijds is net deze delicate belangenafweging het basiskenmerk van elke privacyreglementering en haar toepassing in de praktijk. De relatieve complexiteit van dit vraagstuk is geen reden om af te zien van de waarborgen die onze privacywetgeving te bieden heeft.

⁷⁷ Arrest Niemitz van het Europese Hof voor de Rechten van de Mens, EHRM 16 december 1992, A-251.B., punt 33 (geciteerd in de pre-ambule bij dit hoofdstuk).

⁷⁸ Doch niet op een volledig sluitende manier: indien het de klant is die als eerste een bericht verstuurt naar de werknemer, dan kon de klant vooraf onmogelijk kennis nemen van de disclaimer en is het dus ook betwistbaar of hij zijn toestemming heeft gegeven voor de kennisname van de inhoud ervan door de werkgever.

⁷⁹ Ontwerp van wet ter bescherming van de persoonlijke levenssfeer tegen het beluisteren, kennisnemen en opnemen van privé-communicatie en –telecommunicatie, Parl.St. Senaat 1992-93, nr. 843/1, 8 en nr. 843/2, 10.

Dit lijkt ook de draagwijdte te zijn van de uitzonderingsbepaling van artikel 125, §1 van de WEC: noch artikel 124 van de WEC, noch artikel 259bis en 314bis Sw. zijn van toepassing op handelingen die worden toegelaten of opgelegd door de wet. Hierin kan onder meer een verwijzing worden gelezen naar de relevante bepalingen van de Arbeidsovereenkomstenwet, de Privacywet, CAO 81 en eventueel zelfs het EVRM, die allemaal de kennisname van (het bestaan van) bepaalde telecommunicatieberichten toelaten wanneer aan de hierboven besproken strikte voorwaarden werd voldaan.

Een bijzondere wettelijke toestemming tot kennisname van de communicatie van/naar de werknemers werd ingevoerd via de zogenaamde Pestwet⁸⁰, waarmee de wetgever het mogelijk wilde maken om efficiënter op te treden tegen “mobbing”, het lastigvallen van collega’s in een professionele omgeving. Artikel 5 van deze wet bevat een aantal aanpassingen aan de Welzijnswet van 4 augustus 1996 die de werkgever verplichten om de nodige maatregelen te treffen om efficiënt te kunnen optreden tegen mobbing, zonder evenwel nadrukkelijk naar het telecommunicatiegeheim te verwijzen. Toch heeft de Privacycommissie in een advies van 18 december 2003⁸¹ aangegeven dat deze wet naar haar mening een voldoende grondslag kan zijn om een inbreuk op het telecommunicatiegeheim te verantwoorden⁸².

Ook in het algemeen erkent de WEC dat tijdelijke registratie van professionele communicatie noodzakelijk en toelaatbaar kan zijn om bewijsredenen. Artikel 128 van de WEC functioneert in dat kader als verduidelijking van de Privacywet, door de registratie van elektronische communicatie en de daarmee verband houdende verkeersgegevens uitgevoerd in het legale zakelijke verkeer als bewijs van een commerciële transactie of van een andere zakelijke communicatie toe te staan. De bij de communicatie betrokken partijen moeten dan wel vóór de registratie op de hoogte worden gebracht van de registratie, de precieze doeleinden ervan en de duur van de opslag van de registratie.

Omwille van deze voorwaarden kan het toepassingsgebied van deze uitzondering dus niet worden uitgebreid naar beroepsmatige communicatie in het algemeen, vermits dit ook communicatie omvat die wordt uitgewisseld alvorens de nodige informatie wordt kenbaar gemaakt. Bovendien is opslag van de vermelde gegevens enkel toegelaten tot het einde van de periode waarbinnen de transactie in rechte kan worden aangevochten.

Call centers en kwaliteitscontrole

Er wordt algemeen aanvaard dat bepaalde arbeidsplaatsen omwille van de inhoud van de uitgewisselde berichten een sterkere controle op het telecommunicatieverkeer van de werknemers mogen inrichten. Dit is overigens conform de basisbeginselen van artikel 8 van het EVRM: aangezien proportionaliteit één van

⁸⁰ Wet van 11 juni 2002 betreffende de bescherming tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk, B.S. 22 juni 2002

⁸¹ Zie het advies van de Privacycommissie van 18 december 2003: “Bij afwezigheid van toestemming van de deelnemers aan de communicatie, is kennisname door de werkgever van de door de werknemer gevoerde communicatie enkel mogelijk [onder meer indien] de wet dit toestaat of oplegt. [...] Wanneer er ernstige aanwijzingen zijn dat e-mailberichten worden verstuurd waarvan de inhoud als pesterij, ongewenst seksueel gedrag of enige andere vorm van gewelddadig gedrag kan worden gekwalificeerd, waardoor een accuraat en onpartijdig onderzoek moet worden gevoerd, dan kan de werkgever beroep doen op deze wettelijke bepaling die hem oplegt de nodige maatregelen te treffen teneinde de elektronische communicatie te controleren. Het betreft een belangenconflict, waarbij het belang van het slachtoffer van de pesterijen dient te primeren.”

⁸² Zie hierover in meer detail F.HENDRICKX, Elektronisch toezicht op het werk: Internet en camera’s, Ced.Samsom, Diegem, 2000, p. 94 en volgende.

de criteria is waaraan elke maatregel getoetst moet worden spreekt het voor zich dat activiteiten die een groter risico voor de werkgever inhouden ook aanleiding mogen geven tot een meer verregaande controle.

Het hierboven besproken artikel 128 van de WEC is hiervan een toepassing. Dit artikel verduidelijkt dat tijdelijke registratie van professionele communicatie noodzakelijk en toelaatbaar kan zijn om bewijsredenen. Communicatie in het legale zakelijke verkeer dat moet dienen als bewijs van een commerciële transactie of van een andere zakelijke communicatie mag op grond van dit artikel worden geregistreerd of zelfs opgenomen.

Dit is een belangrijke verduidelijking voor bedrijven die bijzonder afhankelijk zijn van telecommunicatie-technieken voor hun professionele activiteiten, zoals telebankingdiensten of beursbedrijven. Zij kunnen zich immers hierop baseren om een registratie- en opnamebeleid uit te werken. Weliswaar zijn zij niet vrijgesteld van de relevante bepalingen van de Privacywet: alle betrokken partijen (inclusief werknemers en cliënten) moeten onder meer vóór de registratie op de hoogte worden gebracht van de registratie, de precieze doeleinden ervan en de duur van de opslag van de registratie.

Daarbij moeten de geregistreerde gegevens worden gewist wanneer de te bewijzen transactie niet meer in rechte kan worden aangevochten.

Ook voor call centers voorziet artikel 128 van de WEC in een uitzonderingsbepaling: in afwijking van artikel 259bis en 314bis van het Strafwetboek is het kennisnemen en registreren van elektronische communicatie en de verkeersgegevens met als enig doel de kwaliteit van de dienstverlening in call centers te controleren toegestaan. Dit is niet onlogisch: de hoofdfunctie van werknemers in een call center is immers telecommunicatie, zodat een ernstige inperking op de kennisname en registratie van de telecommunicatie de facto zou neerkomen op een evenredige uitsluiting van het toezichtsrecht van de werkgever.

Ook hier moet er nog aan de andere voorwaarden van de Privacywet worden voldaan: de personen die werkzaam zijn in het call center moeten op voorhand op de hoogte worden gebracht van de mogelijkheid tot kennisnemen en registreren, het precieze doel ervan en de duur van bewaring van de geregistreerde communicatie en gegevens. Die gegevens mogen ten hoogste gedurende één maand worden bewaard.

Telewerken: arbeid in de informatiemaatschappij

Basisprincipes en kenmerken

De bovenstaande overwegingen zijn voornamelijk toegespitst op de traditionele arbeidscontext, waarbij een werknemer zich op een locatie bevindt die onder de min of meer rechtstreekse controle van de werkgever staat. Los van deze context groeide er in de voorbije jaren ook een steeds grotere interesse voor een nieuw arbeidsmodel, waarbij de werknemer zijn werk verricht op afstand (d.w.z.: niet op de bedrijfslocatie), daarbij gebruik makend van informatietechnologie die de werkgever tot zijn beschikking stelt: het zogenaamde telewerken.

Telewerken oefent een sterke aantrekkingskracht uit op werkgevers en werknemers. Wanneer de aard van het werk zich daartoe leent, dan kan de werknemer zijn tijd immers veelal efficiënter inrichten, hetgeen ook de werkgever ten goede kan komen. Nochtans levert telewerken ook een aantal specifieke problemen op, waarbij het wegvallen van een duidelijke toezichtsmogelijkheid voor de werkgever één van de grootste juridische en vooral psychologische barrières vormt.

Een regelgevend kader kon dan ook niet lang uitblijven. Op 1 juni 2006 trad CAO 85 van 9 november 2005 betreffende het telewerk dan ook in werking⁸³. Deze CAO, die algemeen verbindend werd verklaard bij kb van 13 juni 2006⁸⁴, regelt een aantal belangrijke discussiepunten, zoals het louter vrijwilliger karakter van telewerken, de verplichting om een aantal essentiële punten schriftelijk vast te leggen, en de kostenvergoeding van de werknemer.

Het regelgevend kader voor telewerken werd vervolledigd door Titel XIII van de Wet van 20 juli 2006 houdende diverse bepalingen⁸⁵, die enkele noodzakelijke aanvullingen aanbracht aan de Arbeidsovereenkomstenwet en aan de Arbeidsreglementenwet; en door CAO 85bis⁸⁶, algemeen verbindend verklaard via een kb⁸⁷ van 19 maart 2008 dat verduidelijkte onder welke omstandigheden er sprake was van een arbeidsongeval bij telewerk. Deze laatste vraag is bij telewerkers immers vaak moeilijk te beoordelen wanneer zij van thuis uit werken, a fortiori wanneer zij bovendien zelf instaan voor hun tijdsindeling. Binnen het kader van dit hoofdstuk zal er enkel worden ingegaan op de draagwijdte en impact van CAO 85.

Bijzondere regels in verband met privacybescherming

Met betrekking tot privacybescherming is de CAO eerder summier, zodat in hoofdzaak de bovenstaande regels van toepassing blijven. Toch zijn er een aantal bijzondere aandachtspunten.

Een eerste probleem is vanzelfsprekend de beschikbaarheid van de werknemer. Het basisbeginsel is dat de telewerker niet korter of langer werkt dan zijn collega's die op de bedrijfslocatie werken. Om die reden zijn werkgever en werknemer dan ook verplicht om in een schriftelijke overeenkomst (de zogenaamde telewerkovereenkomst: hetzij een autonome overeenkomst, hetzij een bijlage bij de bestaande arbeidsovereenkomst) vast te leggen in welke periodes de telewerker geacht wordt beschikbaar te zijn, en op welke wijze (via telefoon, e-mail,...). Op die manier wordt een eerste drempel ingebouwd voor de bescherming van het privéleven van de telewerker: de beschikbaarheid van informatica-infrastructuur in zijn woonst impliceert niet dat hij op elk moment van de dag beschikbaar dient te zijn.

⁸³ Zie <http://www.cnt-nar.be/CAO/cao-85.pdf>

⁸⁴ Koninklijk besluit van 13 juni 2006 waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst nr. 85 van 9 november 2005, gesloten in de Nationale Arbeidsraad, betreffende het telewerk, B.S. 5 september 2006.

⁸⁵ Wet van 20 juli 2006 houdende diverse bepalingen, B.S. 28 juli 2006.

⁸⁶ Collectieve arbeidsovereenkomst 85bis tot wijziging van de collectieve arbeidsovereenkomst nr. 85 van 9 november 2005 betreffende het telewerk, gesloten in de Nationale Arbeidsraad op 27 februari 2008; zie <http://www.cnt-nar.be/CAO/cao-85bis.pdf>

⁸⁷ Koninklijk besluit van 19 maart 2008 waarbij algemeen verbindend wordt verklaard de collectieve arbeidsovereenkomst nr. 85bis van 27 februari 2008, gesloten in de Nationale Arbeidsraad, tot wijziging van de collectieve arbeidsovereenkomst nr. 85 van 9 november 2005 betreffende het telewerk, B.S. 14 april 2008.¹

voetnoot¹ voetnoot

Het tweede probleem is delicaat, en betreft de inrichting van mogelijkheden om toezicht te houden op de activiteiten van de werkgever. Dit probleem wordt gedeeltelijk opgelost (of beter: voorkomen) door het wederzijds vrijwillige karakter van het telewerken: de werknemer kan nooit telewerk eisen, en de werkgever kan dit nooit verplichten. Daardoor speelt vertrouwen een nog belangrijkere rol in telewerken dan in traditionele arbeidsrelaties: indien de werkgever meent dat de prestaties van een werknemer zouden verzwakken zonder toezicht, dan zal hij het verzoek tot telewerken eenvoudigweg weigeren. Telewerkers zijn dan ook idealiter werknemers met de nodige capaciteiten om autonoom te werken, en werknemers waarvan de productiviteit gemakkelijk afgelezen kan worden aan hun output. Met andere woorden: telewerkers moeten grotendeels beoordeeld kunnen worden door toezicht op hun resultaten, eerder dan op de activiteiten die zij daarvoor hebben gesteld.

De voornaamste vragen in verband met privacy stellen zich dan ook met betrekking tot het toezicht op het gebruik van de werkmiddelen door de telewerker. Aangezien telewerken geen bijkomende kosten mag opleveren voor de werknemer krijgt de werkgever de taak om de telewerker van de nodige infrastructuur te voorzien, inclusief door het vergoeden van de communicatiekosten die het telewerken met zich meebrengt. Dit impliceert nochtans niet dat de werkgever zijn telewerkers noodzakelijkerwijs van alle mogelijke infrastructuur (computer, printer, Internetabonnement,...) moet voorzien; wanneer de werknemer zelf al over deze infrastructuur beschikt, dan kan hij eveneens aanbieden om louter de kosten voor het professionele gebruik van deze infrastructuur te vergoeden.

Het toezicht op de werkinfrastructuur wordt daarmee natuurlijk niet eenvoudiger, vermits bijvoorbeeld een computer zowel voor privé- als voor beroepsmatig gebruik bestemd kan zijn. Net als bij andere arbeidssituaties (zie hierboven) is het dan ook vooral van belang om duidelijk met de werknemer af te spreken welk deel van de infrastructuur hij louter beroepsmatig dient te gebruiken en op welke manier deze gecontroleerd kan worden, teneinde de kans op latere discussies te minimaliseren.

De telewerkovereenkomst die verplicht moet worden opgesteld is daarbij een uitstekend vehikel om te herinneren aan het algemeen geldende privacybeleid, en om eventuele bijzondere regels voor thuiswerkers te beklemtonen. Dit is hoe dan ook noodzakelijk, aangezien de CAO eveneens verplicht om mechanismen te voorzien voor de controle van de veiligheids- en gezondheidsmaatregelen op de werkplek. Controles van de werkplek moeten aldus mogelijk zijn, hoewel de werkgever wel verplicht is om deze voorafgaandelijk aan te kondigen en de toestemming van de telewerker te bekomen als de werkplek tevens een woonplaats is (artikel 15 van de CAO). Het spreekt voor zich dat deze bijzondere regels te allen tijde de algemene principes van de Privacywet in acht dienen te nemen.

Het spreekt voor zich dat de telewerker zelf niet de enige is voor wie de thuiswerksituatie privacyrisico's inhoudt. Indien de telewerker betrokken is bij de verwerking van persoonsgegevens – hetgeen vaak het geval is, vermits administratieve functies een groot deel van de thuiswerkers vertegenwoordigen – dan spreekt het voor zich dat de werkgever ook de nodige maatregelen moet nemen om de vertrouwelijkheid en de veiligheid van deze gegevens te verzekeren. De werkgever blijft immers de verantwoordelijke voor de verwerking van deze gegevens, en is dus volgens de Privacywet verplicht om de nodige technische en organisatorische maatregelen te treffen om deze gegevens te beschermen.

Dit impliceert dat de werkgever ervoor zal moeten zorgen dat de persoonsgegevens waarvoor hij verantwoordelijk is afdoende beveiligd zijn tegen beschadiging, vernietiging of verlies; hij kan deze

verantwoordelijkheid niet afwentelen op de telewerker. De CAO bevestigt deze verplichting expliciet in artikel 14. Het gebruik van technische maatregelen zoals versleuteling van vertrouwelijke gegevens, paswoorden voor het opstarten van computersystemen, en frequente back-ups moet daarbij overwogen worden. Hoe grondig deze maatregelen moeten zijn hangt af van geval tot geval, en wordt zoals steeds gedicteerd door de stand van de techniek en de al dan niet privacygevoelige aard van de gegevens.

Aangepast uittreksel van het boek: *"Privacywetgeving in de praktijk"*,
Hans Graux en Jos Dumortier
© Uitgeverij UGA, 2009

Beknopte biografie

Jos Dumortier is al sinds 1981 verbonden aan de K.U. Leuven. Vandaag is hij er behalve hoogleraar ook vice-decaan van de faculteit Rechtsgeleerdheid.

Daarnaast is hij onderzoeksleider in het Interdisciplinair Centrum voor Breedbandtechnologie, Advocaat aan de Balie van Brussel, Voorzitter van de "Legal Interest Group" van EEMA, Bestuurder van FITCE Belgium en tScheme, Lid van het "Observatorium van het Internet" en Editor van de "International Encyclopedia of Cyberlaw", Kluwer International Publishers.

Interdisciplinair Centrum voor Recht en ICT

Jos DUMORTIER is de oprichter en de huidige directeur van het Interdisciplinair Centrum voor Recht en ICT (ICRI). Het ICRI is een expertisecentrum op het gebied van juridische aspecten van informatie- en communicatietechnologie. Het bestaat uit een vaste kern van 25 voltijdse onderzoekers en een groot aantal freelance medewerkers. Het ICRI is een onderzoeksgroep van het Instituut voor Breedbandtechnologie (www.ibbt.be).

time.lex

Onder de naam "time.lex" werkt Jos Dumortier sinds 2007 met een twaalfstal gespecialiseerde partners en medewerkers als advocaat en juridisch raadgever op het domein van het informatie- en technologie recht. Het kantoor time.lex voerde belangrijke opdrachten uit o.m. voor de Europese Commissie, de Federale Overheidsdienst Economie en het Ministerie van de Vlaamse Gemeenschap. De groep heeft een sterke expertise in juridische aspecten van informatiebeveiliging, verwerking van persoonsgegevens, elektronische handtekeningen, elektronische handel en e-government.

LA JURISPRUDENCE BELGE ET LA JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME CONCERNANT LA VIE PRIVÉE AU TRAVAIL

Steve Gilson

Biographie sommaire

Steve Gilson est licencié en droit de l'UCL et licencié en droit social de l'ULG et il est avocat au Barreau de Namur. Après avoir été assistant à la Faculté de droit à l'Université catholique de Louvain pendant 8 ans, il est devenu maître de conférences invité à l'UCL où il enseigne le droit de la sécurité sociale et le droit de la sécurité sociale approfondi. Il est par ailleurs chargé de cours à l'ICHEC où il enseigne le droit social.

ETAT DES LIEUX DE LA VIE PRIVEE AU TRAVAIL A LA LUMIERE DE LA JURISPRUDENCE

Steve GILSON¹

Avocat au Barreau de Namur

Maître de Conférences invité à la Faculté de droit de l'UCL

Chargé de cours à l'ICHEC

OBJET DE LA CONTRIBUTION

1. Objectifs et limite de l'exposé. Notre objectif est de donner, à lumière de la jurisprudence, un état des lieux synthétique de la vie privée au travail. La question est tellement vaste au vu des innombrables situations dans lesquelles elle est susceptible de se poser, qu'il n'est donc nullement question d'exhaustivité ou d'analyse approfondie des sujets traités pour lesquels il sera renvoyés aux publications utiles. Le présent texte est par ailleurs l'état à ce jour d'un travail en « cours de construction » et les auteurs reconnaissent volontiers son caractère parcellaire ou superficiel sur certaines questions.

INTRODUCTION : UNE VIE PRIVEE AU TRAVAIL²

1. DIFFICULTÉ D'UNE DÉFINITION DE LA NOTION DE VIE PRIVÉE

2. La vie privée, une notion évolutive. La notion de « vie privée » visée à l'article 8 de la C.E.D.H.³ est éminemment évolutive et ne se laisse pas enfermer dans une définition stricte : « l'expression *vie privée* est large, ne se prête pas à une définition exhaustive »⁴. La Cour

¹ L'auteur remercie vivement Mme Karen ROSIER pour ses suggestions et commentaires.

² Pour un exposé récent des principes généraux relatifs à la vie privée au travail, voyez : KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XIème colloque de l'association famille et droit, UCL, 30 novembre 2007 ; NEVEN, J.-F., « Les principes généraux : les dispositions internationales et constitutionnelles », in LECLERCQ, J.-F. (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Editions du Jeune Barreau, 2005, spéc., pp. 39-48, n° 31-36. On ne peut que se référer également à la remarquable étude de F. HENDRICKX., *Privacy en arbeidsrecht*, Die Keure, 1999 ; PEIFFER, A., MATTHUS, A. et VERLINDEN, E., *Privacy in de arbeidsrelatie. Gids voor het voeren van een privacybeleid*, STAPPERS, J. (dir.), Gand, Story, 2008, 162 p ; Voyez aussi : DE BAERDEMAEKER, R. et KOKOT, M., « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, 1-13 ; DELARUE, R., « Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven », *Chron. D.S.*, 1992, 133-141 ; Récemment, un numéro spécial d'une revue et un ouvrage ont été consacrés à ce sujet : « L'employeur et la vie privée du travailleur », *Orientations*, 2005, numéro spécial, 1-95 ; *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Editions du Jeune Barreau, 2005

³ Voyez sur ce sujet not. : KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XIème colloque de l'association famille et droit, UCL, 30 novembre 2007, p.1 ; RIGAUX, F., *La protection de la vie privée et des autres biens de la personnalité*, Bruxelles, Bruylant, 1990.

⁴ Cour eur. D.H., arrêt Perry c. Royaume-Uni, 17 juillet 2003, *Rec.*, 2003-IV, § 36, p. 166 ; arrêt Peck. c. Royaume-Uni, 28 janvier 2003, *Rec.*, 2003-I, § 57, p. 183 ; arrêt Pretty c. Royaume-Uni, 29 avril 2002, *Rec.*, 2002-III, § 61, p. 244 ; P.G. et J.H. c. Royaume-Uni, 25 septembre 2001, *Rec.*, 2001-IX, § 56, p. 256

européenne des droits de l'homme revendique ainsi la nécessité d'interpréter l'article 8 selon l'évolution des conditions de vie⁵ dans une optique extensive et non restrictive⁶.

3. Afin de ne pas donner une acceptation trop importante à la notion de « vie privée », dans cette contribution, nous n'aborderons pas la question des droits et libertés autrement protégés comme, par exemple, la liberté des cultes ou la liberté d'association.

2. RECONNAISSANCE D'UNE VIE PRIVÉE AU TRAVAIL

4. La vie privée et la vie professionnelle ne s'opposent pas. Dans son désormais célèbre arrêt *Niemitz c. Allemagne*, la Cour européenne des droits de l'homme a considéré que : « *le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la « vie privée » comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur* »⁷.

La Cour de cassation française, dans son arrêt *Nikon* du 2 octobre 2001, sur la base de l'article 8 de la C.E.D.H., considère que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* »⁸.

Il n'est pas inutile de rappeler sociologiquement les mélanges de temps de vie professionnels et privés comme la question des gardes à domiciles ou des exigences de disponibilité posées aux salariés⁹.

5. Le droit au respect de la vie privée peut par ailleurs être revendiqué même dans un espace public. Si « *la surveillance des faits et gestes d'une personne dans un lieu public au moyen d'un dispositif photographique ne mémorisant pas les données visuelles ne constitue pas en elle-même une forme d'ingérence dans la vie privée, en revanche, le fait de recueillir systématiquement de telles données et de les mémoriser peut soulever des questions liées à la vie privée* »¹⁰. Dans cette hypothèse, néanmoins, la légitime attente d'un droit au respect de la vie privée doit être envisagée différemment. La vie privée ne s'exerce pas de la même manière chez soi, en rue ou au travail.

⁵ Cour eur. D.H., arrêt société Colas c. France, 16 avril 2002, *Rec.*, 2002-III, §41, p. 123.

⁶ Arrêt Amann c. Suisse, 16 février 2000, *Rec.*, 2000-II, § 65, p. 81.

⁷ Arrêt Niemitz c. Allemagne du 16 décembre 1992, *J.T.*, 1994, p. 65 et note JAKHIAN. Voyez aussi Cour eur. D.H., arrêt Halford c. Royaume-Uni du 25 juin 1997, *Rec.*, 1997-III, p. 1016, § 43-45 ; arrêt Amann c. Suisse du 16 février 2000, *Rec.*, 2000-II, p. 224, § 65 ; *R.W.*, 2002-2003, p. 235 ; arrêt Rotaru c. Roumanie du 4 mai 2000, *Rec.*, 2000-V, p. 80, § 43.

⁸ Arrêt Nikon, Cass. Fr., 2 octobre 2001, *Chron. D.S.*, 2002, p. 242 ;

⁹ MOULY, J., « Vie professionnelle et vie privée. De nouvelles rencontres sous l'égide de l'article 8 de la Convention européenne », in SUDRE, F., (éd.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2005, pp. 280 et s.

¹⁰ Cour eur. D.H. arrêts Perry c. Royaume-Uni, § 38 ; Rotaru c. Roumanie, § 43 ; Amann c. Suisse, § 65.

6. La vie privée peut donc s'exercer au travail et dans les locaux de son employeur. Jugé ainsi par la Cour européenne des droits de l'homme « *qu'il ressort clairement de sa jurisprudence que les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de vie privée et de correspondance visées à l'article 8, § 1* »¹¹.

Nous verrons par ailleurs qu'un effet direct horizontal peut être donné l'article 8 (Voyez *infra*).

3. NÉCESSITÉ DE LA RECHERCHE D'UN ÉQUILIBRE ENTRE LE POUVOIR DE SURVEILLANCE DE L'EMPLOYEUR ET LA VIE PRIVÉE DU TRAVAILLEUR

7. Equilibre délicat entre droits antagonistes. Nous verrons que le droit de surveillance de l'employeur est reconnu. La recherche d'un équilibre entre les droits antagonistes amène à de délicates balances d'intérêts qui expliquent la jurisprudence très variable rendue à ce sujet.

CHAPITRE I : QUELQUES PARTICULARITES DE LA VIE PRIVÉE EN DROIT DU TRAVAIL

1. ABSENCE DE NORME GÉNÉRALE PROPRE AU TRAVAIL QUI CONSACRE LA VIE PRIVÉE DU TRAVAILLEUR

8. Le droit du travail belge ne comporte pas une règle générale consacrant la vie privée du travailleur. La Constitution consacre le droit au respect de la vie privée en son article 22, qui dispose que : « *Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit* ». Il ne s'agit toutefois pas d'une norme propre au droit social ou qui aborde spécifiquement la protection de la vie privée dans ce cadre particulier.

9. Il existe des règles spécifiques de protection de la vie privée. Nous verrons qu'il existe une multitude de dispositions spécifiques de protection de la vie privée – propre ou non au droit social - dans certaines circonstances et que, par ailleurs, de nombreuses dispositions du droit social ont été créées dans un souci de protection de celle-ci. On aura égard, notamment, à la loi du 8 décembre 1992 concernant la protection de la vie privée dans le cadre de l'utilisation de données à caractère personnel¹², à la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, aux dispositions relatives à l'installation et

¹¹ Cour eur. D.H., Arrêt Halford, 25 juin 1997, *Rec.*, 1997, III, p.1016

¹² PLASSCHAERT, E. et DELCORDE, J., "Le traitement et la protection des données personnelles des travailleurs", *Orientations*, 2005, numéro spécial, 25-40 ; E. PLASSCHAERT, « La protection des données personnelles dans le cadre du contrôle des prestations de travail », in *Vie privée du travailleur et prérogatives patronales*, Ed. du Jeune Barreau de Bruxelles, 2005, p. 97 ; S. GILSON, « Introduction, spécificité et enjeu de la protection des données à caractère personnel dans les relations de travail », in *Défis du droit à la protection de la vie privée, perspectives du droit européen et nord américain*, M. V. PEREZ ASINARI et P. PALAZZI (ed.), Bruxelles, Bruylant, 2008

l'utilisation de caméras de surveillance (loi du 21 mars 2007), à la surveillance par caméras sur le lieu de travail (C.C.T. n° 68 du 16 juin 1998), au contrôle de l'utilisation d'internet et des courriels sur le lieu de travail (C.C.T. n° 81 du 26 avril 2002), au contrôle d'accès et de sortie des travailleurs (C.C.T. n° 89 du 30 janvier 2007), à la mise en œuvre d'une politique préventive en matière d'alcool et de drogues dans l'entreprise, en ce compris les tests de dépistage (C.C.T. n° 100 du 1^{er} avril 2009). La conjonction des règles issues des conventions collectives de travail avec les autres dispositions est souvent malaisée. Ainsi, par exemple, la convention collective de travail n° 100 pose-t-elle des problèmes de compatibilité avec la loi du 8 décembre 1992 ou l'Arrêté royal du 28 mai 2003.

10. En-dehors des règles spécifiques, il faut recourir aux principes généraux issus de l'interprétation des articles 8 de la C.E.D.H. Pour tous les sujets qui font l'objet d'une réglementation spécifique en droit belge, à la supposer conforme aux exigences de l'article 8, il n'y a, en théorie, plus lieu de se référer à cette disposition sauf si elle apporte des garanties supérieures à la norme nationale vu sa primauté de norme supranationale. Nous verrons toutefois que la jurisprudence de la Cour européenne des droits de l'homme peut être un guide précieux dans les balances d'intérêts que le juge est souvent amené à faire en la matière. Les partenaires sociaux, lorsqu'ils ont dû intervenir, dans les matières touchant la vie privée des travailleurs ont systématiquement mis en place des modalités de compromis afin d'assurer un juste équilibre entre le droit à la surveillance de l'employeur et le droit à la vie privée du travailleur. On y retrouve fréquemment l'usage du principe de finalité, celui de proportionnalité et celui de transparence. C'est particulièrement net dans la convention collective de travail n° 68 ou dans la convention collective de travail n° 81 par exemple. Par ailleurs, dans les hypothèses où la loi belge ne régit pas spécifiquement une question précise, l'article 8 de la Convention européenne des droits de l'homme continue de rester un référent incontournable. Parmi les questions générales qui ne font pas l'objet d'une réglementation spécifique et qui doivent être envisagées par rapport au principe de base, figure notamment la question des fichiers qui seraient sauvegardés sur le disque dur d'un ordinateur mis à disposition du travailleur dans l'entreprise.

2. RÉGLEMENTATION DE DIFFÉRENTES PROBLÉMATIQUES PAR LE RECOURS À DES CONVENTIONS COLLECTIVES DU TRAVAIL¹³

11. L'autonomie des partenaires sociaux et le recours aux CCT. En Belgique, l'autonomie des partenaires sociaux amène fréquemment à ce que la régulation des rapports de travail nécessitant des équilibres entre droit de contrôle de l'employeur et vie privée du travailleur¹⁴ se fasse par le biais de convention collective de travail. Cela a notamment été le cas pour l'usage des caméras (C.C.T. n°68), des technologies de communication électroniques (C.C.T. N°81) ou encore de l'usage de drogue ou d'alcool (C.C.T. 100) Le choix d'une convention

¹³ Cette section est issue de : S. GILSON, *L'alcool et les drogues dans l'entreprise*, Vanden Broele, 2009

¹⁴ Sur la vie privée du travailleur, voyez not. HENDRICKX, F., *Privacy en arbeidsrecht*, n°1 de *Bijzondere reeks ICA*, Bruges, La Charte, 1999, 358 p; DE BAERDEMAEKER, R. et KOKOT, M., « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, 1-13 ; DELARUE, R., « Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven », *Chron. D.S.*, 1992, 133-141. ; GOLDFAYS, M. et VAN MOORSEL, L., « Quelques aspects de la protection de la vie privée du travailleur à l'égard de son futur employeur », *Orientations*, 2002, 189-208.- ; LAGASSE, F., « La vie privée et le droit du travail », *Chron. D.S.*, 1997, 417-434; J.-F. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Ed. J.B.B., Bruxelles, 2005; Numéro spécial d'*Orientations*, 35 ans, 2005; DE SCHUTTER, O., « La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi », *Rev. trim. D.H.*, 2003, liv. 54, p. 654.

collective – nécessaire si les partenaires sociaux souhaitent régler eux-mêmes une problématique – entraîne deux conséquences évidentes que nous nous contenterons de rappeler.

12. L'exclusion du secteur public. La convention collective de travail, source de droit, issue de la loi du 5 décembre 1968, fut-elle intersectorielle comme c'est le cas en l'espèce, ne touche pas l'ensemble des travailleurs. En effet, la loi du 5 décembre 1968 exclut de son champ d'application (art. 2, § 3) les personnes qui sont occupées, pour parler bref et de façon très schématique, par un employeur du secteur public et ce, même si elles sont occupées dans un contrat de travail. Comme le relève Jean Jacqmain : «*Sauf dans les rares exceptions qui assujettissent les institutions publiques à la législation privée, la convention collective de travail n'existe pas dans le secteur public* »¹⁵. Le secteur public connaît, en effet, un système de relations collectives tout à fait particulier¹⁶.

Dès lors, à supposer les conventions collectives inapplicables si l'employeur se situe hors du champ d'application de la loi, il faudra se référer aux autres textes qui régissent éventuellement la problématique. A défaut, à supposer qu'il n'y ait pas d'autres textes spécifiques applicables, par exemple dans le statut particulier du personnel dont question, il faudra se référer essentiellement à l'article 8 de la Convention européenne des droits de l'homme en invoquant son effet direct, vertical dans ce cas. L'absence éventuelle d'intervention législative dans le secteur public entraîne dès lors une dualité de règles applicables dont la constitutionnalité pourrait être interrogée. A défaut de dispositions spécifiques dans le statut, il n'est pas certain que des instruments purement privés puissent pallier une telle absence de réglementation légale ou compléter.

13. Ingérence dans la vie privée – nécessité d'une loi – hiérarchie des sources. Il est possible de s'interroger sur l'opportunité d'avoir autorisé (et limité) des ingérences à la vie privée par des conventions collectives de travail alors que l'on sait que tant l'article 22 de la Constitution que l'article 8 de la Convention européenne des droits de l'homme exigent que les ingérences dans la vie privée aient une *base légale*. S'il a été relevé qu'au sens de l'article 8 de la Convention européenne des droits de l'homme le terme « loi » pouvait désigner toute « norme de droit interne, écrite ou non pour autant que celle-ci soit accessible et prévisible »¹⁷ il est souligné par contre que la Constitution exige un acte qui émane du pouvoir législatif¹⁸.

¹⁵ J. JACQMAIN, « Les relations collectives dans le secteur public », in *Une terre de droit du travail : les services publics*, (dir), Bruxelles, Bruylant, 2005, p. 395.

¹⁶ C. DUMONT, « Les relations collectives de travail dans la fonction publique », in M. DUMONT (dir), *Le droit du travail dans tous ses secteurs*, Anthemis, 2008, p. 401 et s.

¹⁷ J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Ed. Jeune Barreau de Bruxelles, 2005, p. 29.

¹⁸ E. DEGRAVE, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.*, 2009, p. 366 ; B. DOCQUIR, *Le droit de la vie privée*, Larcier, De Boeck, 2008, p.105 ; J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Ed. Jeune Barreau de Bruxelles, 2005, p. 30. Désireux de contourner l'obstacle, certains estiment que lorsqu'il n'y a pas de norme spéciale, il serait possible de se fonder sur le principe général d'autorité de l'employeur sur le travailleur concrétisé par l'article 17, 2° de la loi du 3 juillet 1978 relative aux contrats de travail (Voyez par exemple T. CLAEYS, « L'utilisation des nouvelles technologies et de l'e-mail durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *Le contrat de travail et la nouvelle économie*, Ed. du jeune barreau de Bruxelles, 2001, p. 265). Il n'est pas exclu qu'une telle interprétation puisse être retenue, pour certaines ingérences si on se place sous l'angle de l'article 8 de la C.E.D.H. quoique alors le problème pourrait se poser plutôt en terme de prévisibilité lorsque la norme est très vague. Par contre, il est inutile de rappeler qu'une norme d'une telle généralité ne saurait suffire aux critères de l'article 22 de la Constitution. Un contrat de travail ou un règlement de travail sont certainement plus précis mais

Sans doute serait-il possible de considérer que la C.C.T. 100 ne ferait ici que mettre en œuvre en pratique un principe de prévention générale inscrit dans la loi¹⁹ mais il faudrait constater rapidement que la norme d'habilitation, à supposer qu'une telle habilitation soit possible²⁰, ne vise pas une ingérence dans la vie privée.²¹ Il est donc envisageable, en théorie, de critiquer sur cette base les obligations qui naissent de ces sources.²²

De plus, une convention collective de travail, de par sa place inférieure dans la hiérarchie des sources, ne peut déroger à une loi. Or, le problème se pose fréquemment (Voyez not. dans la C.C.T. 81 ou la C.C.T. 100). La convention collective de travail, norme emblématique de l'autonomie des partenaires sociaux, présente donc à ce sujet un deuxième inconvénient, le premier étant de ne pas s'appliquer à l'ensemble des employeurs.

3. PROBLÉMATIQUE DU CONSENTEMENT DU TRAVAILLEUR DANS UN CONTRAT INÉGALITAIRE

14. Du consentement en droit social. De nombreuses dispositions se réfèrent à celui-ci lorsqu'il est exigé²³ ou encore, simplement pour vérifier l'acceptation par le travailleur de règles relatives à la surveillance. La problématique de la possibilité d'un consentement libre du travailleur est presque aussi ancienne que le droit social. Nonobstant l'inégalité économique et juridique entre les parties, le principe de la possibilité d'un consentement doit être reconnu à peine de nier même l'existence du contrat de travail. Reste à savoir comment, dans ce contexte, le consentement peut être libre et éclairé et, surtout, spécifique à un acte de surveillance. D'ordinaire, le consentement se donne *ex ante* par l'approbation d'un règlement de travail ou d'une charte d'utilisation. Certaines décisions se contentent du consentement implicite du travailleur pour considérer que la preuve n'a pas été obtenue illicitement²⁴. Un consentement spécifique au moment des faits est sans doute souhaitable mais le travailleur risque de le refuser ou d'être soumis à une pression²⁵.

La question du consentement a nécessité dans certains cas un cadre réglementaire spécifique. Ainsi, par exemple, certaines données à caractère personnel sensibles²⁶ peuvent être traitées

se heurterait tout autant à l'exigence de légalité qui, selon la Cour constitutionnelle implique « *que les règles soient adoptées par une assemblée délibérante, démocratiquement élue* » (Voy. Not. C.A., 19 juillet 2005, n° 131/2005, www.courconstitutionnelle.be).

¹⁹ Comp. Pour d'autres dispositions : O. MERENO et .S. VAN KOEKENBEEK, « Les mutations de la vie privée au travail », *Orientations*, 2005, p. 17

²⁰ Or, une telle habilitation est exclue (Voyez sur ce point, J.-F. NEVEN, *op. cit.*, pp.30 et s.)

²¹ J.-F., NEVEN, *op.cit.*, p. 36.

²² Voyez à ce sujet J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Ed. Jeune Barreau de Bruxelles, 2005, p. 34 et s.

²³ Voyez par exemple l'article 124 de la loi du 13 juin 2005 sur les communications électroniques.

²⁴ C. T. Anvers (sect. Anvers), 8 janvier 2003, *Chr. D.S.*, 2003 ; p.193 ; *R.W.*, 2005-2006, p. 391.

²⁵ C.T. Bruxelles, 13 septembre 2005, *Computerr.* 2006, p. 100. La Commission de la Protection de la Vie Privée avait également mis en cause le caractère libre du consentement de l'employé lorsque celui-ci pour utiliser l'internet – à quelque fin, personnelle ou professionnelle, que ce soit – n'a pas d'autre choix que de cliquer sur le bouton d'acceptation des conditions imposées par l'employeur afin d'avoir accès au réseau (Commission de la Protection de la Vie Privée, Avis n°13/03 sur le contrôle par l'employeur des données de communication de l'un de ses employés, 27 février 2003, www.privacycommission.be).

²⁶ A savoir, les données à caractère personnel relatives à la santé ainsi que celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale et les données relatives à la vie sexuelle.

avec le consentement *écrit* de la personne concernée. L'article 1, § 8 de la loi du 8 décembre 1992 qui transpose l'article 2, h) de la directive 95/46/CE énonce les exigences que le consentement de la personne concernée doit rencontrer: celui-ci doit être libre, spécifique et informé. Il en résulte, tout d'abord, que le consentement doit être donné sans pression, qu'il s'agisse d'une pression économique ou morale. Ensuite, le consentement ne peut être général : il doit porter sur des traitements spécifiquement définis notamment par rapport à leurs finalités. Enfin, le consentement doit être donné en connaissance de cause, sur la base d'une information qui permette à la personne concernée d'analyser les risques d'atteinte à ses droits et libertés que le ou les traitements peuvent entraîner. Ceci implique que la personne ait au minimum reçu les informations exigées aux termes de la loi de 1992 (en son article 9) et dans l'arrêté royal du 13 février 2001²⁷. Par ailleurs, il nous semble important de rappeler que la personne concernée peut retirer son consentement à tout moment et sans devoir justifier ce retrait²⁸. Les conséquences d'un tel retrait seront que le responsable du traitement ne pourra plus traiter les données relatives à la santé, pour l'avenir, sur la base de l'exception du consentement.

On pressent immédiatement que la condition du libre consentement peut paraître utopique dans le contexte d'une relation de travail, tout comme dans le contexte d'un entretien d'embauche d'ailleurs. Le législateur en a tenu compte puisqu'il stipule à l'article 27 de l'Arrêté royal du 13 février 2001 que le traitement des dites données sensibles sur la seule base du consentement écrit de la personne concernée lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement l'empêchant de refuser librement son consentement. Dans une telle situation, le consentement écrit permet néanmoins le traitement s'il s'agit d'octroyer un avantage à la personne concernée. Cette disposition a été critiquée du fait qu'elle peut laisser penser qu'un consentement non libre sur le un traitement présentant toutefois un avantage, même minime, pour le travailleur constituerait un fondement valable²⁹.

C'est une des premières fois, à notre sens, où l'on reconnaît de façon claire que le consentement ne puisse pas être donné librement dans une situation où il y a une subordination économique. En effet, dans l'analyse civiliste classique, le fait que le travailleur se trouve dans une position économiquement plus faible ne suffit pas à considérer que son accord est vicié de ce fait³⁰ sauf à démontrer l'abus d'une position dominante. La Cour de cassation belge a ainsi décidé que « *de la seule circonstance que la défenderesse est une partie « économique faible », il ne saurait se déduire que son consentement a été obtenu à la suite d'erreur, de violence ou de dol et que, par conséquent, il n'était pas valable (....) d'autre part, il ne ressort d'aucune disposition légale que le consentement donné à une convention par une partie économiquement faible est toujours dénué de validité* »³¹. S'il n'y a donc pas existence d'un vice propre, il convient également de relever que la même

²⁷ Th. LEONARD, « La protection des données à caractère personnel et l'entreprise » in *Le guide juridique de l'entreprise*, Titre XI, Livre 112.1, Bruxelles, 2^{ème} éd., Kluwer, p. 20.

²⁸ M.-H. BOULANGER, S. CALLENS et St. BRILLON, « La protection des données personnelles relatives à la santé et la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998 et complétée par l'arrêté royal du 13 février 2001 », *Rev. Dr. Santé*, 2000-2001, p.335.

²⁹ Th. LEONARD, *ibidem*, p. 38.

³⁰ C.Trav. Mons, 4 décembre 2000, *inédit*, R.G. 15181

³¹ Cass., 2 mai 1969, *Pas.*, 1969, I, p.781.

circonstance ne fait pas présumer le dol ou la violence³². Ce principe, fermement établi³³, est à la fois *élémentaire*³⁴ -puisque si l'inverse était vrai, le travailleur ne pourrait conclure un quelconque contrat de travail, ni effectuer valablement aucune renonciation dans la plupart des hypothèses- et *particulièrement crucial* puisqu'il s'agit d'une réalité indéniable qui, dans les faits, se révèle fort présente et, en droit, apparaît comme en filigrane dans les dispositifs ponctuels de protection du consentement du travailleur.

Si, en droit interne, l'association des droits de l'homme avec le concept d'ordre public est fréquente³⁵ (les droits de l'homme sont indérogeables et ne peuvent faire l'objet de renonciation car ils sont « inaliénables et sacrés »³⁶, extra-patrimoniaux³⁷ indépendamment d'une quelconque référence à l'ordre public³⁸), une analyse détaillée de la jurisprudence de la Cour européenne des droits de l'homme, telle celle menée par P. Frumer, démontre qu'est inexacte l'idée que l'appartenance éventuelle de la Convention européenne des droits de l'Homme et des libertés fondamentales à l'ordre public, et même à un ordre public européen, fasse nécessairement obstacle à la possibilité d'une renonciation³⁹ même si la Cour européenne des droits de l'homme estime que la nature de certains droits reconnus par la Convention fasse obstacle à une renonciation⁴⁰. Ainsi, quelles que soient les difficultés de dégager des critères cohérents dans la jurisprudence de la Cour⁴¹, en se plaçant dans le cadre de la C.E.D.H., « *l'autonomie de la volonté semble justifier que l'acceptation d'une fonction ou la conclusion d'un contrat puisse aboutir à une limitation consentie desdits droits et libertés* », le travailleur pouvant à terme mettre fin à cet emploi⁴². D'où la nécessité de protections spécifiques du consentement.

A notre sens, à l'heure actuelle, si la règle est suffisamment précise sur les modalités du contrôle (et que celui-ci est évidemment licite au regard d'un texte spécifique ou des principes généraux de finalité, proportionnalité et légalité) et portée à connaissance du travailleur en temps opportun (par le règlement de travail), le consentement du travailleur doit être considéré comme valable. Il faut néanmoins apporter une attention toute particulière à la vérification de cet élément vu le contexte de la relation de travail. On notera toutefois que la

³² Trib. trav. Bruxelles, 5 septembre 1988, *J.T.T.*, 1988, p.446

³³ C. trav. Mons, 30 juin 1988, *J.T.T.*, 1988, p.376 ; Trib. Trav. Liège, 11 juin 1991, *J.T.T.*, 1992, p.23, Trib. trav. Bruxelles, 3 septembre 1990, *J.T.T.*, 1991, p.13 ; C.Trav. Mons, 30 juin 1988, *Chron.D.S.*, 1989, p.135, *J.T.T.*, 1988, p.376, *Bull. F.E.B.*, 1990, p.378

Voyez la jurisprudence française relatée in G. LOISEAU, « L'application de la théorie des vices du consentement au contrat de travail » in *Etudes offertes à J. GHESTIN. Le contrat au début du XXI^e siècle*, L.G.D.J., 2001, pp.584-585

³⁴ Il s'agit en fait et en droit de la survie de la fiction de l'égalité contractuelle et, partant, du maintien d'une conception contractuelle du contrat. Sur cette question : M. JAMOULLE, *Le contrat de travail*, Tome I, Faculté de Droit, d'Economie et de Sciences sociales de Liège, Liège, 1982, p.282

³⁵ P. FRUMER, *La renonciation aux droits et libertés. La Convention européenne des droits de l'homme à l'épreuve de la volonté individuelle*, Bruxelles, Bruylant, 2001, p.486

³⁶ G. GRAMMATIKAS, *Théorie générale de la renonciation en droit civil (Etude parallèle du droit français et du droit hellénique)*, Paris, L.G.D.J., 1971, p.50

³⁷ G. GRAMMATIKAS, *ibidem*, p.76

³⁸ En faveur de cette thèse : G. GRAMMATIKAS, *ibidem*, pp.50-51.

³⁹ P.FRUMER, *op. cit.*, p.505

⁴⁰ P.FRUMER, *op. cit.*, pp.260-261.

⁴¹ F.OST et S. VAN DROOGHENBROECK, « La responsabilité, face cachée des droits de l'homme » in E.BRIBOSIA et L.HENNEBEL (sous la direction de), *Classer les droits de l'homme*, Bruylant, Bruxelles, 2004, p.131

⁴² P.FRUMER, *op.cit.*, p.637

question de savoir si le règlement de travail peut valoir preuve du consentement donné par le travailleur à une ingérence de la vie privée est discutée⁴³.

4. PLACE DES CONVENTIONS PARTICULIÈRES RELATIVES À LA VIE PRIVÉE ET DU RÈGLEMENT DE TRAVAIL

15. Règlements particuliers. On relèvera que ce soit dans le secteur privé ou dans le secteur public⁴⁴ qu'à notre sens, la prolifération des chartes, règles déontologiques, protocoles, etc. ne sauraient avoir d'effet contraignant pour le travailleur que s'ils figurent dans le contrat de travail ou le règlement de travail (qui doit comporter notamment les droits et obligation du personnel de surveillance).

CHAPITRE II : L'ARTICLE 8 C.E.D.H.⁴⁵ COMME CADRE DE REFERENCE GENERAL

16. L'article 8 et le droit à la vie privée. La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales a été adoptée le 4 novembre 1950 par le Conseil de l'Europe et est entrée en vigueur le 3 septembre 1953⁴⁶. L'article 8 de la Convention stipule :

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

⁴³ Voyez à ce sujet J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Ed. Jeune Barreau de Bruxelles, 2005, pp. 44 et 45.

⁴⁴ J. JACQMAIN, « Extension des règlements de travail à l'ensemble des services publics », *Chron. D.S.*, 2001, p. 65 et s. ; C. DRESSEN, « L'obligation d'établir un règlement de travail dans le secteur public », in J. JACQMAIN, *Une terre de droit du travail : les services publics*, actes du colloque organisé à Genvall le 10 novembre 2005 par la Conférence du Jeune Barreau de Nivelles et l'Association des juristes praticiens du droit social, Bruylant, 2005, p. 31 et s.

⁴⁵ DE SCHUTTER, O., et VAN DROOGHENBROECK, S., *Droit international des droits de l'homme devant le juge national*, Bruxelles, Larcier, 1999, spéc. pp. 210-212 ; VAN DROOGHENBROECK, S., « L'horizontalisation des droits de l'homme », in DUMONT, H., OST, F. et VAN DROOGHENBROECK, S., *La responsabilité face cachée des droits de l'homme*, Bruxelles, Bruylant, 2005, spéc. p. 371 et note 59 ; MOULY, J., « Vie professionnelle et vie privée. De nouvelles rencontres sous l'égide de l'article 8 de la Convention européenne », in SUDRE, F., (éd.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, 2005, pp. 279-303, spéc. n° 30 à 33) ; DE HERDT, P., *Artikel 8 EVRM en het Belgisch Recht. De bescherming van privacy, gezin, woonst en communicatie, C.D.P.D.-Libri*, vol. 4, Gand, Mys & Breesch, 1998 ; DE HERT, P., « Artikel 8. Recht op privacy », in VANDE LANOTTE, J. et HAECK, Y., *Handboek EVRM, Deel 2. Artikelsgewijze commentaar*, Anvers, Intersentia, 2004, pp. 705-788 ; SUDRE, F., *Droit international et européen des droits de l'homme*, 8° éd., Paris, P.U.F., 2006 ; SUDRE, F., (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruxelles, Bruylant, Némésis, 2005 ; SUDRE, F. (dir.), *Le droit au respect de la vie familiale au sens de la Convention européenne des droits de l'homme*, Coll. Droit et Justice, n° 38, Bruxelles, Némésis, Bruylant, 2002 ; VAN DROOGHENBROECK, S., « La Convention européenne des droits de l'homme (1999-2001) », *Dossiers du J.T.*, n° 39, Bruxelles, Larcier, 2003 ; VELU, J. et ERGEC, R., *La convention européenne des droits de l'homme, R.P.D.B., Complément VII*, Bruxelles, Bruylant, 1990.

⁴⁶ Ratifiée par la Belgique le 14 juin 1955, elle a fait l'objet d'une loi d'approbation du 13 mai 1955 (*Mon.*, 19 août 1955, *Errat.*, *Mon.*, 29 juin 1961), entrée en vigueur le 19 août 1955.

2. *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ».

Il est admis que la plupart des dispositions de la Convention, d'ordre public, ont un effet direct en droit belge⁴⁷ et priment donc sur le droit national⁴⁸. L'article 8 C.E.D.H. peut donc être invoqué :

- d'une part, en l'absence de texte spécifique, comme cadre général de référence. Comme le relève J.-F. NEVEN « *Certaines situations qui, selon la conception que l'on s'en fait, débouchent sur une ingérence dans la vie privée des travailleurs ne sont pas expressément réglementées. En l'absence de norme spécifique, le juge peut envisager d'appliquer un principe général (tel que le principe de l'exécution de « bonne foi ») ou de faire une application directe de l'article 8 de la C.E.D.H.* »⁴⁹.
- d'autre part, même en présence de règles nationales spécifiques si celles-ci s'avéraient moins protectrices puisque la C.E.D.H. a effet direct.

Un effet d'horizontalisation des droits de l'homme est relevé de sorte que les dispositions de l'article 8 sont invocables dans les relations entre particuliers.

17. Limites au droit à la vie privée et conditions. Toutefois, le droit au respect de la vie privée n'est pas un droit absolu. Ainsi, l'article 8 al.2 de la Convention dispose que «*Il ne peut y avoir ingérence d'une autorité publique*⁵⁰ *dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui*».

Toute ingérence dans la vie privée d'un individu n'est donc pas légitime : certaines conditions doivent pour cela être vérifiées.

* L'ingérence doit tout d'abord être prévue par une loi qui soit suffisamment précise, claire, accessible et prévisible⁵¹. C'est le principe de légalité. Cette condition signifie qu'en dehors d'une autorisation légale, tout acte d'ingérence dans la vie privée d'autrui est contraire à l'article 8 de la Convention européenne des droits de l'homme. La notion de « loi » doit toutefois être entendue de manière très large : au sens de l'article 8 de la Convention européenne des droits de l'homme (et au contraire de ce que vise l'article 22 de la

⁴⁷ VELU, J. et ERGEC, R., « La convention européenne des droits de l'homme », *R.P.D.B.*, Complément VII, Bruxelles, Bruylant, 1990, n° 99 ; Cass., 10 mai 1985, *Pas.*, 1985, I, p. 1122

⁴⁸ Cass., 27 mai 1971, *Pas.*, 1971, I, p. 886

⁴⁹ Op.cit., p. 30, n° 38

⁵⁰ Malgré ce libellé, cet article s'applique également aux relations nouées entre particuliers et donc aux relations entre employeur et travailleur (J. VELU et R. ERGEC, *La convention européenne des droits de l'homme*, op. cit., p. 533). Nous aborderons infra l'effet horizontal de la C.E.D.H.

⁵¹ Notamment : Cour eur. D. H., arrêt *Sunday Times* du 26 avril 1979, Série A, n°30, §49.

Constitution) le terme « loi » pouvait désigner toute « norme de droit interne, écrite ou non pour autant que celle-ci soit accessible et prévisible »⁵². Un contrat de travail, un règlement de travail, un règlement particulier peuvent, par exemple, constituer une telle base à l'aune de l'article 8 C.E.D.H. mais évidemment pas au regard de l'article 22 de la Constitution. Du reste, il ne nous semble pas que le seul art. 17, 2° de la loi du 3 juillet 1978 puisse l'être à défaut de prévisibilité de l'ingérence⁵³. Or, il s'agit finalement de la seule base légale consacrant l'autorité de l'employeur (et donc son pouvoir de surveillance) qui pourrait être invoquée pour justifier les ingérences non réglées par un texte spécifique (quoi que de nombreuses ingérences soient réglées elles-mêmes par des CCT).

* L'ingérence doit, en outre, poursuivre un des buts légitimes limitativement énoncés dans l'alinéa 2 de l'article 8 de la Convention européenne des droits de l'homme. Parmi ceux-ci figurent notamment la protection des droits et libertés d'autrui ainsi que la protection de la santé. C'est le principe de finalité. À cet égard, il semble difficilement soutenable que des préoccupations de rentabilité et de compétitivité puissent à elles seules être invoquées par l'employeur pour justifier une ingérence dans la vie privée du candidat au travail. Elles ne correspondent, en effet à aucun critère de l'article 8 al. 2. Comme le souligne M. Vincineau : *« Des intérêts strictement matériels ne sont pris en compte que lorsque la Convention en a expressément décidé : ainsi, dans le Protocole additionnel n°1 relatif à la propriété privée. L'inverse reviendrait à saper l'édifice des droits fondamentaux au nom du profit et à nier leur caractère inaliénable »*⁵⁴. Toutefois, comme le relève J.-F. NEVEN, il s'agit de concepts très larges et la « protection des droits et libertés d'autrui » peuvent certainement intégrer le droit de l'employeur au respect du contrat.

* Enfin, l'ingérence doit être une mesure « *nécessaire, dans une société démocratique, à la poursuite de ce but* ». Ceci implique qu'en plus d'être utile au but poursuivi, l'ingérence considérée soit la mesure la moins dommageable pour la réalisation de ce but. En outre, la Cour européenne des droits de l'homme a décidé, dans l'arrêt *Olsson c. Suède* : « ...la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et notamment proportionné au but légitime recherché... »⁵⁵. Il s'agit de vérifier « si un juste équilibre a été ménagé entre ce but et le droit en cause, tenant compte de son importance et de l'intensité de l'atteinte portée »⁵⁶. C'est le principe de proportionnalité⁵⁷.

Comme le souligne J.-F. NEVEN, « A l'occasion de ce contrôle de proportionnalité, des intérêts patrimoniaux ou économiques peuvent être mis en balance avec le droit au respect de la vie privée »⁵⁸ : la primauté des droits fondamentaux n'est donc pas absolue ». Cet auteur cite

⁵² J.-F. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, Ed. Jeune Barreau de Bruxelles, 2005, p. 29.

⁵³ Voyez sur cette question : KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XIème colloque de l'association famille et droit, UCL, 30 novembre 2007, pp.5 et 6.

⁵⁴ M. VINCINEAU, « Assurance et vie privée. Du vide légal à l'illicite », *R.B.D.I.*, 1994/2, p. 486 ; dans le même sens : F. RIGAUX, « La protection des droits de la personnalité », in *Colloque du Centre de bioéthique de l'U.C.L.*, 1988, t. II, p. 140.

⁵⁵ Cour eur. D.H., arrêt *Olsson c. Suède* du 24 mars 1988, Série A, n° 130, p. 31-32, par. 67 ; Cour eur. D.H., arrêt *Dudgeon* du 22 octobre 1981, série A, p. 15, § 51.

⁵⁶ V. COUSSIRAT-COUSTERE, « Article 8 §2 », in », in *La convention européenne des droits de l'homme. Commentaire article par article*, sous la direction De L.-E. PETTITI E. DECAUX et P.-H. IMBERT, *op. cit.*, p. 338.

⁵⁷ Cass. 23 janvier 1991, *Pas.*, 1991, I, 491.

⁵⁸ Voir aussi Cass. 29 janvier 1999, *Bull.*, 1999, p. 111 : l'ingérence ne doit pas nécessairement viser à garantir des droits fondamentaux.

l'arrêt *Verlière* de la C.E.D.H. qui valide le recours à un détective privé par un assureur⁵⁹. Des impératifs de sécurité peuvent aussi être avancés. Dans deux arrêts, la Cour - consacrant indirectement un effet horizontal de la Convention européenne des droits de l'homme⁶⁰ - applique un « principe de proportionnalité privatisée »⁶¹ aux ingérences de l'employeur dans le droit au respect de la vie privée⁶² :

- dans son arrêt *Madsen* du 7 novembre 2002⁶³, la Cour avait à connaître de la situation d'un garçon de cabine employé sur un Ferry danois qui avait dû fournir un échantillon d'urine dans le cadre d'un contrôle de détection de drogues organisé par son employeur en vertu du règlement de travail. La Cour considère qu'eu égard à la spécificité du modèle danois de l'organisation du travail, une telle réglementation peut se faire par le biais d'une convention collective de travail et par le biais d'un règlement émis sur cette base. La Cour va dès lors considérer que le règlement a été émis sur base du droit de l'employeur à contrôler le travail et avait un objectif légitime visant la sûreté publique et la protection des droits de liberté d'autrui..
- Dans l'arrêt *Wretlund* du 9 mars 2004, une travailleuse faisant partie du personnel de nettoyage d'une centrale nucléaire avait du également se soumettre à des tests de dépistage de drogues et d'alcool dans le cadre de prélèvement d'urine. La Cour va considérer que même si l'obligation, en vertu de laquelle les salariés devaient se soumettre à des tests de dépistage de drogues, ne résultait pas de la législation, le droit pour l'employeur de définir et d'organiser le travail constituait un principe généralement accepté sur le marché du travail suédois. L'atteinte à l'intégrité a été estimée également légitime eu égard aux circonstances particulières de l'espèce et, notamment, les règles de sécurité publique.

Conformément aux critères de l'article 8, dans les deux hypothèses, la Cour européenne des droits de l'homme retient en tous cas l'idée d'une transparence de ce type de contrôle (prévue chaque fois dans un règlement) et d'une finalité, en l'espèce de sécurité publique. Mais la sécurité des travailleurs ou des tiers pourraient, nous semble-t-il, justifier une telle ingérence dans d'autres milieux professionnels. Aux yeux de l'article 8 de la C.E.D.H., une réglementation contenue dans une C.C.T. remplit parfaitement la condition de légalité telle que précisée, par exemple, dans l'arrêt *Sunday Times*⁶⁴.

⁵⁹ Décision *Verlière c. Suisse*, 28 juin 2001, *Rec.*, 2001-VII, p. 411.

⁶⁰ Sur ce sujet, voyez : V. VAN DER PLANCKE et N. VAN LEUVEN, « La privatisation du respect de la Convention européenne des droits de l'homme : faut-il reconnaître un effet horizontal généralisé ? », *CRIDHO Working Paper*, 2007, n° 3, p. 23 disponible sur http://cridho.cpd.r.ucl.ac.be/documents/Working.Papers/CRIDHO_WP_2007-3.pdf.

⁶¹ A. CARILLON, « Les sources européennes des droits de l'homme salarié », Bruxelles, Bruylant, 2006, p. 111 ; voy. aussi à ce sujet, « L'entreprise et la convention européenne des droits de l'homme », P. de FONTBRESSIN, Bruxelles, Bruylant, 2008.

⁶² J.-P. MARGUENAUD et J. MOULY, « L'alcool et la drogue dans les éprouvettes de la C.E.D.H. : vie privée du salarié et principe de proportionnalité » in *Recueil Dalloz*, 2005, p. 36 et s. Voyez également, à ce sujet : « Convention européenne des droits de l'homme et droit du travail », J.-P., MARGUENAUD et J. MOULY, Exposé du 21 mars 2008 à l'association française des droits du travail et de la sécurité sociale ; J.-E., RAY, « Drogues dans l'entreprise », *Vie des entreprises. Chronique juridique. Liaisons sociales*, Novembre 2005, p. 58 et s.

⁶³ Cour eur. D.H., 7 novembre 2002, *NjW*, 2003, 376, note E.V.B.

⁶⁴ Cour eur. D.H., 26 avril 1979, *Sunday Times*, N°6538/74, *Rec.*, Série A, vol. 30, p.31

Dans l'arrêt *Copland* du 3 avril 2007⁶⁵, la Cour Européenne des Droits de l'Homme a déclaré fondée la plainte portée par une employée d'une école privée britannique contre son employeur en raison de la surveillance systématique de l'emploi d'internet, des *e-mails* et du téléphone (not. via les factures de téléphone) par ce dernier sans avertissement préalable. La Cour indique expressément ne pas exclure qu'une disposition légale puisse autoriser le recours à des moyens de surveillance visant l'emploi des moyens de communications utilisés par les travailleurs mais estime que, en l'espèce, mais considère, dans l'espèce, que ces contrôles ne sont pas prévus par une loi conforme aux exigences de l'article 8, §2.

18. Difficulté d'application des critères. Comme le souligne J.-F. NEVEN, « *La démarche est relativement lourde. Un test complet de conformité implique, à tout le moins, que le juge vérifie « l'applicabilité » de l'article 8 de la C.E.D.H., en précisant en quoi il estime que la situation litigieuse constitue une ingérence dans la vie privée du travailleur ; qu'il vérifie si cette ingérence a été autorisée par le travailleur ou dispose d'une base légale suffisante (« accessible » et « précise ») ; qu'il examine si cette ingérence répond aux principes de finalité et de proportionnalité, en tenant compte de l'ensemble des éléments du contexte (nature des activités de l'entreprise, responsabilités particulières du travailleur, nature exacte du travail ...)* ».

CHAPITRE III : LA VIE PRIVÉE DANS LA PHASE PRE-CONTRACTUELLE⁶⁶

19. La C.C.T. n°38 et la protection de la vie privée. La convention collective de travail n° 38 du 6 décembre 1983, concernant le recrutement et la sélection des travailleurs, régit la période précontractuelle durant laquelle l'employeur va sélectionner et recruter des travailleurs⁶⁷. L'article 11 de la C.C.T. 38 consacre le respect de la vie privée du candidat. Cette disposition va servir de cadre à la réflexion sur les questions qui peuvent être posées aux candidats par l'employeur lors du recrutement. Des questions relatives à la vie privée des travailleurs ne peuvent être posées que si elles sont pertinentes en raison de la nature et des conditions d'exercice de la fonction. On retrouve donc les critères de l'article 8 de la Convention européenne des droits de l'homme.

20. Obligation d'information⁶⁸ ? Si la question est légitime et pertinente par rapport aux exigences de la fonction, l'employeur peut la poser, le travailleur ne peut pas refuser d'y répondre et s'il ment, il commet un dol. Les parties ont en effet dès le stade de la formation du contrat (négociation), une obligation d'information l'une envers l'autre. Cette obligation

⁶⁵Cour eur. D.H., arrêt *COPLAND* du 3 avril 2007, <http://www.echr.coe.int/echr/>. Voyez sur cet arrêt : K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail » (Chronique de jurisprudence en droit des technologies de l'information (2002-2008)), *R.D.T.I.*, 2009, n° 35,

⁶⁶ Certaines parties de ce chapitre sont issues de S. GILSON, *Syllabus de droit social*, ICHEC, 2009 (syllabus réalisé en collaboration avec N. HAUTENNE)

⁶⁷ MAIRY, C. « Protection de la vie privée dans le cadre du recrutement et de la sélection », *Orientations*, 2005, 5, 18-24 ; GOLDFAYS, M. et VAN MOORSEL, L., « Quelques aspects de la protection de la vie privée du travailleur à l'égard de son futur employeur », *Orientations*, 2002, 189-208.

⁶⁸ Sur ce sujet, voyez not. : HAUTENNE, N., ROSIER, K. et GILSON, S., « Les informations médicales dans la relation de travail », *Orientations*, 2005, numéro spécial, 61-95 ; KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XIème colloque de l'association famille et droit, UCL, 30 novembre 2007, pp.21 et s.

d'information découle d'une obligation de bonne foi. Le dol est en quelque sorte le manquement d'une partie à son obligation d'information au stade pré contractuel.

Si la question n'est pas légitime et/ou pertinente, l'employeur ne peut pas la poser et s'il la pose, le travailleur peut refuser d'y répondre ou y mentir, constituant en quelque sorte une exception aux devoirs du candidat prévus aux articles 13 et 14 de la C.C.T. 38 qui est tenu de collaborer de bonne foi à la procédure de sélection et de fournir toutes les données nécessaires quant à son passé professionnel et aux études qu'il a effectuées, dès lors que cela a un rapport avec la nature et les conditions d'exercice de la fonction.

Le Tribunal du travail de Gand a dans un jugement du 18 mai 1981⁶⁹ résumé les principes d'information qui sont applicables en vertu de l'obligation de bonne foi. Chaque partie a le devoir d'informer l'autre dans certaines limites :

- 1° celui qui détient l'information doit savoir ou est censé savoir que l'autre partie attache de l'importance à cette information⁷⁰ ;
- 2° l'autre partie n'a pas connaissance de cette information et ne pouvait pas l'avoir ;
- 3° le détenteur de l'information doit lui-même être au courant de l'information demandée ;
- 4° l'information demandée ne doit pas être du domaine de la vie privée⁷¹ ;
- 5° les informations demandées ne peuvent avoir pour conséquence qu'elles conduisent à un refus d'engagement contraire à la loi⁷².

21. Applications - Etat de santé. Il va donc être, en général, considéré que le travailleur n'a pas l'obligation d'informer le futur employeur d'une maladie ou d'un handicap, sauf si cela constitue un danger pour la sécurité du travailleur, ses collègues ou des tiers⁷³ ou que c'est de nature même à compromettre la réalisation même du travail⁷⁴. Il est généralement admis que l'employeur peut solliciter des informations médicales lorsque celles-ci sont nécessaires à la détermination de l'aptitude au travail et à la protection de la santé et de la sécurité du futur travailleur ou des tiers⁷⁵. Précisons encore que le principe de proportionnalité exige que ces informations soient non seulement utiles et nécessaires à la poursuite de la finalité envisagée mais encore que la collecte de ces informations soit la mesure la moins intrusive ou dommageable pour atteindre ce but. Notons enfin que cette collecte se fait par l'intermédiaire du médecin du travail qui est soumis au secret médical envers l'employeur.

22. Applications - Etat de grossesse. L'état de grossesse de la travailleuse relève de la vie privée et ne doit pas être communiquée à l'employeur. Par ailleurs, elle pourrait donner lieu à un refus d'embauche illégal, soit constitutif de discrimination⁷⁶. On reconnaît généralement à

⁶⁹ Trib. trav. Gand, 18 mai 1981, *R.W.*, 1981-82, 1426 cité in W. VAN EECKHOUTTE, *Compendium droit socia 200ç-2010, droit du travail*, T.1, Kluwer, p.556

⁷⁰ Ce qui implique que l'information doit être utile au regard de la fonction. L'information pertinente est donc celle qui a un lien utile avec la fonction.

⁷¹ Certaines informations qui pourraient être utiles à l'employeur ne sont donc pas légitimes.

⁷² On vise notamment un refus d'embauche d'une femme enceinte ou, plus généralement, tous les critères de discrimination (Voyez L. 10 mai 2007).

⁷³ C.T. Bruxelles, 5 novembre 1997, *J.T.T.*, 1998, p. 183

⁷⁴ Trib. trav. Courtrai, 13 octobre 1981, *Jura Falc.*, 1981-1982, p. 294.

⁷⁵ cfr alinéa 2 de l'article 8 de la Convention européenne des droits de l'homme

⁷⁶ Trib. trav. Gand, 18 mai 1981, *R.W.*, 1981-82, 1426 ; voy. aussi : C. trav. Anvers, 25 mai 1990, *Chron. D.S.*, 1995, 223, note H. FUNCK et J. JACQMAIN, *C.J.C.E.*, 8 novembre 1990, *J.T.T.*, 1991, 122

la femme enceinte non seulement le droit de se taire si cette question lui est posée et sans que l'employeur ne puisse ultérieurement invoquer le dol mais également le droit de mentir à propos de son état⁷⁷. Notons toutefois que l'information relative à l'état de grossesse doit être communiquée si la candidate postule à un emploi impliquant des conditions particulières qui peuvent s'avérer dangereuses pour la femme enceinte ou pour le fœtus et qui justifie un écartement de celle-ci. Dans ce cas, l'employeur est fondé à solliciter des informations sur l'état de grossesse de la candidate. Dans cette hypothèse, la Cour de justice a néanmoins décidé que : « *La directive 76/207/Ce s'oppose au refus d'engager une travailleuse enceinte pour une durée indéterminée au motif qu'une interdiction légale fait obstacle, pour la durée de sa grossesse, à ce qu'elle occupe cet emploi dès le départ*⁷⁸ ».

23. Applications - Condamnations. La jurisprudence considère généralement que le travailleur doit mentionner une condamnation pénale si cela lui est demandé et qu'il ne peut mentir à ce sujet⁷⁹. Toutefois, à défaut de demande de l'employeur, s'il n'est pas prouvé que la conclusion du contrat dépendait de la possession d'un casier judiciaire vierge, le consentement de l'employeur n'est pas vicié et il ne peut pas être reproché au travailleur d'avoir agi par dol⁸⁰. Comme l'a relevé K. Rosier, « *Un extrait de casier judiciaire contient non seulement des données à caractère personnel ordinaire (nom, prénom, adresse,...) mais également des données que l'on qualifie de données judiciaires au sens de l'article 8, § 1^{er} de la loi du 8 décembre 1992, dès lors qu'elles sont relatives des condamnations ayant trait à des infractions. En vertu de cette disposition, le traitement de ces données est, en principe, interdit sauf dans le cadre d'exceptions qui sont énumérées limitativement par l'article 8, § 2 de la loi du 8 décembre 1992* »⁸¹. La commission pour la protection pour la vie privée a d'ailleurs indiqué, dans un avis qu'elle a remis le 11 février 2002⁸², « *de manière générale, il n'est pas permis aux employeurs de récolter et de conserver des certificats de bonne vie et mœurs, même vierges, de leurs employés, sauf si la profession exercée par ces employés est une profession réglementée qui nécessite un casier judiciaire vierge ou exempt de certaines condamnations (fonctionnaires, militaires, agents de gardiennage, avocats, ...)* ».

24. Applications - Confession religieuse. Ces informations relèvent de la vie privée du candidat et du principe de la liberté de culte. Elles ne peuvent donc pas être sollicitées lors de la conclusion d'un contrat de travail. La pratique du culte en tant que telle ne peut être considérée comme une faute, sous réserve qu'elle se concilie avec une exécution correcte du travail convenu⁸³.

25. Applications - Informations relatives à l'affiliation à un parti politique ou à un syndicat Il s'agit d'une question illicite exerçant une coercition sur la liberté d'association⁸⁴.

26. La loi du 28 janvier 2003 relative aux examens médicaux. On peut également aborder, dans la phase précontractuelle, la loi du 28 janvier 2003 relative aux examens médicaux dans

⁷⁷ F. LAGASSE, « La vie privée et le droit du travail », *Chr. D.S.*, 1997, p. 417-435

⁷⁸ C.J.C.E., 3 février 2000, *J.T.T.*, 2000, 121

⁷⁹ C. trav. Anvers, 20 novembre 1991, *Chron. D.S.*, 1992, 123, note

⁸⁰ C. trav. Gand (sect. Bruges), 17 octobre 1984, *Chron. D.S.*, 1986, 167

⁸¹ K. ROSIER, « Contrat de travail et certificat de bonne vie et mœurs : le point », *B.S.J.*, n° 372, 2007, p. 6.

⁸² Avis n° 08/2002 relatif aux traitements de données à caractère personnel réalisés par les sociétés privées d'interim, www.privacycommission.be

⁸³ Voyez Trib. trav. Nivelles, le 11 mars 1994, *J.L.M.B.*, 1994, 1400

⁸⁴ C.E., 3 février 1967, *R.D.S.*, 1967, 252, avis DIDERICH et note M. MAGREZ, Trib. trav. Bruxelles, 5 novembre 1973, *R.D.S.*, 1974, 137

le cadre des relations de travail⁸⁵. Le principe défini par la loi est que l'examen médical ou les informations sollicitées sur l'état de santé ne peut être effectué pour d'autres considérations que celles tirées des aptitudes actuelles et des caractéristiques spécifiques du poste à pourvoir. On peut ainsi, notamment, interdire ainsi l'examen génétique prévisionnel et les tests de dépistage de l'infection par le HIV⁸⁶.

CHAPITRE IV : LA VIE PRIVÉE DANS L'EXECUTION DU CONTRAT

1. LES OBLIGATIONS DES TRAVAILLEURS ET DES EMPLOYEURS EN RAPPORT AVEC LA VIE PRIVÉE

27. Des dispositions éparses révélant le souci de la protection de la vie privée. La loi du 3 juillet 1978, si elle ne contient pas une disposition spécifique à la vie privée du travailleur, contient diverses dispositions qui montrent que le législateur a intégré des préoccupations de cet ordre.

28. Interdiction de certaines clauses. L'article 36 dispose que : « *Sont nulles les clauses prévoyant que le mariage, la maternité ou le fait d'avoir atteint l'âge de la pension légale ou conventionnelle mettent fin au contrat.* ». La Cour de cassation a jugé que l'article 36 visait aussi les clauses qui, indirectement, stipulaient que le mariage de l'employé mettait fin à la convention⁸⁷. On notera incidemment que la jurisprudence condamne les clauses résolutoires qui sont contraires aux dispositions impératives mais aussi qui aboutissent à vider celles-ci de tout sens. Une clause résolutoire qui érigerait en motif de rupture un fait de la vie privée pourrait se trouver condamnée de la sorte dès lors que ce fait de la vie privée se verrait protégé (maternité, crédit-temps,...). *A contrario*, un employeur pourrait prévoir que la déchéance du droit de conduire soit une condition résolutoire pour un chauffeur.

29. Respects et égards mutuels. L'article 16 de la loi du 3 juillet 1978 dispose que travailleur et employeur se doivent le respect et des égards mutuels. Il a déjà été jugé, avant l'entrée en vigueur de la C.C.T. 68, que le contrôle des travailleurs au moyen d'une caméra vidéo portait atteinte au respect de la vie privée auquel le travailleur avait droit et violait ainsi l'article 16 de la loi du 3 juillet 1978⁸⁸.

30. L'obligation de secret des affaires à caractère confidentiel. L'article 17, 3° de la loi du 3 juillet 1978 dispose, notamment, que le travailleur doit se garder tant durant la durée du contrat qu'après la cessation de celui-ci, de divulguer les secrets de fabrication ou d'affaire ainsi que le secret de toute affaire à caractère personnel ou confidentiel dont il aurait eu connaissance dans l'exécution de son activité. C'est une disposition qui, d'une certaine façon,

⁸⁵ Sur cette question, voyez not. : HAUTENNE, N., « Les examens médicaux liés à la relation de travail : bref commentaire de la loi du 28 janvier 2003 », *Rev. dr. Santé*, 2003-2004, 220-224; PLETS, I., « Medische onderzoeken op het werk », *N.J.W.*, 2003, 618-621; SMEESTERS, B. et MORENO, O., « Les examens médicaux au travail », *Orientations*, 2004, 1, 15 à 23 ; VANACHTER, O., « Nieuwe regelgeving over het welzijn op het werk », *Or.*, 2004, 26-30 ; G. DOMEZ, « Le droit au respect de la vie privée dans le cadre des tests préalables à l'embauche », in *Vie privée du travailleur et prérogatives patronales*, Ed. du Jeune Barreau de Bruxelles, 2005, p. 55.

⁸⁶ C.J.C.E., 5 octobre 1994, *Chron. D.S.*, p. 10, note J. JACQMAIN.

⁸⁷ Cass., 25 juin 1979, *Pas.*, 1979, Tome I, p. 1234 ; *J.T.T.*, 1981, p. 72.

⁸⁸ T.T. Bruxelles, 26 mars 1990, *Chron. D.S.*, 1992, p. 154.

peut venir en appui de la protection de la vie privée en interdisant, par exemple, au travailleur de divulguer des données concernant ses collègues de travail qu'il serait amené à traiter (données relatives à la rémunération, par exemple).

31. Les devoirs du culte. L'article 20, 5° de la loi du 3 juillet 1978 dispose que l'employeur doit donner au travailleur le temps nécessaire pour remplir les devoirs de son culte ainsi que les obligations civiques résultant de la loi. Le travailleur peut donc revendiquer l'exercice des devoirs du culte sur les lieux mêmes du travail.

32. Clause d'exclusivité et vie après le travail. On pourrait considérer que la vie « après » le travail soit de la vie privée à l'égard de l'employeur même s'il s'agit d'activités professionnelles. A les supposer non concurrentielles, ces activités sont possibles. Comme le souligne M. JAMOULLE, il découle de cette dernière disposition que : « *le salarié reste libre, sa prestation accomplie, de se livrer à une autre activité dont l'objet est étranger à celui de l'entreprise patronale* »⁸⁹. Une clause d'exclusivité est une clause par laquelle le travailleur s'engage à exercer l'ensemble de ses activités professionnelles au service de l'employeur et à n'exercer aucune autre fonction, ni en qualité de travailleur salarié, ni en qualité d'indépendant. En vertu de la liberté du travail, est nulle une clause d'exclusivité générale selon laquelle le travailleur ne pourrait exercer aucune activité en dehors de celle qui fait l'objet du contrat de travail⁹⁰. Toutefois, une limitation partielle était jugée possible. Une partie de la jurisprudence considère en effet qu'une telle clause pourrait être valide dans la mesure où la clause vise à protéger l'intérêt légitime de l'employeur à une exécution correcte des prestations de travail convenues⁹¹ soit, finalement, pour faire respecter le prescrit de l'article 17 de la LCT. La jurisprudence récente de la Cour de cassation est susceptible de modifier ces conceptions. La Cour a décidé « *La liberté d'exercer une activité professionnelle rémunérée ne peut subir d'autres restrictions que celles qui sont prévues par la loi. Une convention qui, en dehors des cas où la loi l'autorise, a pour but de permettre à l'une des parties d'empêcher l'autre partie d'exercer librement son activité professionnelle, a une cause illicite et est frappée de nullité absolue* »⁹². Puisque l'on ne se trouve pas dans un cas autorisé par la loi, la clause d'exclusivité serait donc nulle dès lors qu'elle a pour effet d'empêcher le travailleur d'exercer une autre activité lucrative.

2. LA SURVEILLANCE DE LA SANTÉ DU TRAVAILLEUR⁹³

33. Surveillance de la santé et protection de la vie privée. L'Arrêté royal du 28 mai 2003 régit la surveillance de la santé du travailleur ; il doit être conjugué avec la loi du 28 janvier 2003 dont nous avons déjà parlé. Les garanties qui encadrent la désignation et le travail du conseiller en prévention, médecin du travail participent, tout comme la finalité de la politique de prévention, à la protection de la vie privée du travailleur. L'article 79, § 2 de l'Arrêté royal prévoit que le traitement des données médicales à caractère personnel, des données d'exposition à des fins de recherche scientifique, d'enregistrement épidémiologique,

⁸⁹ M. JAMOULLE, *Le contrat de travail*, t. II, Liège, 1986, p. 44.

⁹⁰ C. trav. Liège, 15 juin 1983, *J.T.T.*, 1984, 485 ; C. trav. Liège, 19 juin 1985, *J.T.T.*, 1985, 470 ; C. trav. Bruxelles, 21 juin 1988, *Chron. D.S.*, 1989, 135 ; C. trav. Mons, 21 mars 1988, *J.T.T.*, 1988, 160

⁹¹ C. trav. Bruxelles, 6 mai 1981, *R.D.S.*, 1982, 36 ; C. trav. Liège, 15 juin 1983, *J.T.T.*, 1984, 484

⁹² Cass. (3^e ch.), 29 septembre 2008, RG n° 06443.F ; *J.T.T.* 2008, p. 464 et obs. M-L Wantiez ; *J.T.* 2008, p. 699.

⁹³ Sur ce sujet, voyez not. : N. HAUTENNE, K. ROSIER et S. GILSON, « Les informations médicales dans la relation de travail », *Orientations*, 2005, numéro spécial, 61-95

d'enseignement et de formation continue doit respecter les conditions et les modalités prévues par la loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

3. LA SURVEILLANCE PAR L'EMPLOYEUR⁹⁴

34. Principes généraux. Le contrat de travail crée un lien de subordination du travailleur à l'employeur et corrélativement une autorité de celui-ci. L'exercice de cette autorité comprend un pouvoir de direction et de contrôle⁹⁵. Même s'il est admis que l'autorité ne doit pas nécessairement être exercée de manière permanente et effective, il faut que l'employeur soit en mesure d'exercer effectivement son autorité⁹⁶. A côté de cet élément issu du contrat lui-même, le travailleur est le plus souvent occupé au sein de l'entreprise de l'employeur et utilise le plus souvent le matériel mis à sa disposition par celui-ci. L'employeur, titulaire du droit de propriété, a donc un droit de regard sur l'usage de ce matériel. Enfin, l'employeur se voit imposer une responsabilité particulière du fait des actes de ses préposés. Il est logique, également, dans ses conditions qu'il puisse exercer une surveillance de ceux-ci. En conclusion, si le travailleur a incontestablement droit à une vie privée au travail, l'employeur a tout aussi droit à un pouvoir de surveillance du travailleur.

La question qui va se poser de manière aigüe est la recherche d'un équilibre entre ces deux droits antagonistes, recherche qui va souvent passer par une nécessaire réflexion sur les *moyens mis en œuvre*, par l'employeur, pour assurer la surveillance du travailleur. Dans certains cas, les partenaires sociaux ont trouvé un compromis qui a fait l'objet d'une convention collective de travail. Cela n'en signifie pas pour autant que tous les problèmes sont résolus mais il y a déjà quelques balises permettant d'apprécier la régularité du contrôle. Dans d'autres cas, le moyen de contrôle n'a pas fait l'objet d'une réglementation particulière et dans cette hypothèse, il faut s'en référer aux principes généraux et l'article 8 de la Convention européenne des droits de l'homme.

35. La surveillance par camera (C.C.T. 68)⁹⁷ - La convention collective de travail énumère des finalités de la surveillance par caméra. On y trouve la sécurité, la santé, la protection des biens de l'entreprise, le contrôle du processus de production mais également le contrôle du travail du travailleur, tout en précisant qu'il ne peut s'agir que d'une surveillance temporaire

⁹⁴ Certaines parties de cette section sont issues, remaniées, de : S. GILSON, K. ROSIER et E. DERMINE, « La preuve en droit social », in *La preuve, questions spéciales*, CUP, F. KUTY et D. MOUGENOT (dir.), Anthémis, 2008, pp. 179 et s. et K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail » (*Chronique de jurisprudence en droit des technologies de l'information (2002-2008)*), *R.D.T.I.*, 2009, n° 35, pp. 126 et s. ; Pour une chronique de jurisprudence consacrée à la problématique de la vie privée dans les relations de travail, voy. : R. DE BARDEMAEKER et M. KOKOT, « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, pp. 1 à 13

⁹⁵ Cass., 18 mai 1980, *Arrêt Cass.*, 1980-1981, p. 1080.

⁹⁶ Cass., 3 février 2003, *R.W.*, 2004-2005, p. 437, note P. HUMBLET.

⁹⁷ DE HERT, P., DE SCUTTER, O. et SMEESTERS, B., « Emploi, vie privée et technologies de surveillance. A propos de la convention collective de travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail », *J.T.T.*, 2001, 1-12 ; DELARUE, R. et WEYNS, M., « De C.A.O. nr. 68 beschermt de persoonlijke levenssfeer ten opzichte van de camerabewaking op de arbeidsplaats », *Or.*, 1999, 25-32 ; HENDRICKX, F., *Electronisch toezicht op het werk : internet en camera's*, in *Sociale praktijkstudies*, Malines, Kluwer, 2005, 197 ; PATERNOSTRE, B. et VERBRUGGE, F., « Protection de la vie privée et surveillance par caméras sur le lieu de travail », *Orientations*, 1998, 229-230 ; DE HERT, P., « Camera's in befrijven », *Or.*, 1996, 200-208 ; GURWIRTH, S., « Camera's en de noodzakelijke ontgroening van de privacywet », *R.W.*, 1994-1995, 105-113.

lorsque les finalités de contrôle du processus de production qui porterait sur les travailleurs ou de contrôle du travail du travailleur seraient visées. Une surveillance permanente du travailleur, à ce titre, est donc jugée excessive (Voyez aussi l'arrêt C.E.D.H. *Copland* précité). La convention collective de travail prévoit une procédure d'information des travailleurs quant à l'introduction de son mode de surveillance (art. 9 de la CCT). Les conditions de conservation de l'image sont également prévues (art. 12 et 13 de la CCT).

La loi du 8 décembre 1992 reste également applicable à la vidéosurveillance⁹⁸.

36. La surveillance de l'utilisation de l'internet et des courriels (C.C.T. 81)⁹⁹ - Comme le relève K. ROSIER¹⁰⁰, « *Contrairement au courrier papier protégé par le secret des lettres¹⁰¹, le courrier électronique relève du secret des communications électroniques. Outre l'application des articles 8 de la C.E.D.H. et à l'article 22 de la Constitution, on relève que la jurisprudence évoque l'application de l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques¹⁰² (anciennement, article 109terD de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques) et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Le contenu du courrier électronique est toujours protégé par les articles 314bis et 259bis du Code pénal qui n'ont pas été abrogés lors de l'adoption de la nouvelle loi du 13 juin 2005. Toutefois, cette protection n'intervient que pendant la transmission et ces dispositions ont donc une pertinence limitée dès lors que les contrôles interviennent généralement postérieurement à la transmission¹⁰³. A ce cadre légal non spécifique au secteur des relations de travail, est venue s'ajouter en 2002 la Convention collective de travail n°81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau¹⁰⁴. Cette C.C.T. n°81 entend définir dans quelles*

⁹⁸ T.T. Liège (10^{ème} ch.), 10 mars 2005, RG 330.744, *inédit*. Pour une autre application de la loi du 8 décembre 1992 dans un cas de vidéosurveillance, voy. : C.T. Anvers (sect. Hasselt), 6 janvier 2003, *R.W.*, 2003-2004, p. 300; *Chr. D.S.*, 2003, p. 19.

⁹⁹ K. ROSIER, « Le cybercontrôle des travailleurs contrôlé par le Juge », *Orientations*, 2009, n° 6, pp. 22-26S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage de nouvelles technologies », in *Vie privée du travailleur et prérogatives patronales*, Ed. du Jeune Barreau de Bruxelles, 2005, p. 139 ; BLANPAIN, R. et VANGESTEL, M., *Gebruik en controle van e-mail, intranet en internet in de onderneming*, Bruges, La Charte, 2003, 264 p. ; HENDRICKX, F., *Elektronisch toezicht op het werk : internet en camera's*, Malines, Kluwer, 2005, 197 p. ; DE HERT, P., « C.A.O. nr. 81 en advies nr. 10/2001 over controle van internet en e-mail. Sociale herlezen stafwetten en grondrechten », *R.W.*, 2002-2003, 1281-1294 ; DEJONGHE, D., « Wergeverscontrole op e-mail en internetgebruik : C.A.O. nr. 81 slechts de krijtlijn », *Or.*, 2002, 225-235 ; GOLDFAYS, M., « C.C.T. n°81 : contrôle des données de communications électroniques », *Orientations*, 2002, 209-212 ; RIJCKAERT, O., « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, numéro spécial, 41-60.

¹⁰⁰ K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail » (Chronique de jurisprudence en droit des technologies de l'information (2002-2008)), *R.D.T.I.*, 2009, n° 35,

¹⁰¹ Certaines décisions citent cependant l'article 29 de la Constitution comme étant pertinent dans le cadre d'un contrôle de la correspondance réalisée par *e-mail* (voy. : T. T. Liège (3^{ème} ch.), 3 septembre 2008, RG 371.015, www.cass.be, T.T. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be; T.T. Verviers (1^{ère} ch.), 20 mars 2002, *J.T.T.*, 2002, p. 183).

¹⁰² *Mon.b.*, 20 juin 2005, p. 28070.

¹⁰³ Pour des applications de ce principe, voy. : C.T. Anvers (sect. Hasselt), 2 septembre 2008, RG.2070230, *inédit*.; C.T. Anvers (sect. Hasselt), 8 janvier 2003, *Chr. D.S.*, 2003, p. 193; *R.W.*, 2005-2006, p. 391; T.T. Bruxelles (3^{ème} ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61.

¹⁰⁴ Convention collective de travail n°81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, adoptée le 26 avril 2002 et rendue obligatoire par arrêté royal du 12 juin 2002.

conditions un contrôle des données (à l'exclusion du contenu des communications) peut intervenir ».

Partant du compromis de base (les travailleurs ont un droit à la vie privée dans le cadre de la relation de travail mais l'employeur dispose de droit de contrôle), la convention collective de travail n°81 reprend le principe des finalités, le principe de proportionnalité et le principe de transparence. La convention crée également un système d'individualisation des données de communication électroniques en réseau. La procédure est particulièrement complexe et sa mise en œuvre fort délicate, elle ne permet, en théorie, pas, à l'employeur, d'obtenir le contenu de la communication.

La multiplication de normes régissant ces questions, normes souvent fort complexes, explique une jurisprudence très variable qui omet bien souvent un contrôle de légalité à l'aune de toutes les dispositions (not. la Loi du 8 décembre 1992¹⁰⁵). On y retrouve bien souvent un contrôle, à la lumière de l'article 8 de la C.E.D.H., de légalité, de proportionnalité¹⁰⁶ et de finalité, le Tribunal du travail de Hasselt a eu égard à la circonstance que le portable de l'employé¹⁰⁷.

Une multitude de distinctions apparaissent dans la jurisprudence sans nécessairement avoir toujours de fondements légaux clairs et, par exemple :

- l'ordinateur est accessible à tous, sans codes d'accès, et les messages seraient donc par nature publics¹⁰⁸.
- il faudrait distinguer contrôle fortuit¹⁰⁹ et contrôle intentionnel¹¹⁰
- il faudrait distinguer *e-mails* professionnels des courriers privés en considérant que les *e-mails* adressés via une adresse de messagerie professionnelle ont *a priori* un caractère professionnel¹¹¹.

Des décisions surprenantes, qui font manifestement une interprétation erronée des dispositions légales, surgissent également ; de sorte qu'il est aujourd'hui devenu extrêmement difficile de trouver une sécurité juridique à ce sujet¹¹².

37. Fouille, contrôle d'accès et de sortie (C.C.T. 89)¹¹³ - La convention collective de travail n° 89 concerne exclusivement les contrôles de sortie des travailleurs. Pour le contrôle d'accès,

¹⁰⁵ Voyez toutefois T.T. Liège, (10^{ème} chambre), 24 février 2005, RG 327.207, inédit. ; C.T. Bruxelles, 8 avril 2003, *Chr. D.S.*, 2005, p. 208.

¹⁰⁶ T.T. Hasselt (1^{ère} ch.) 21 octobre 2002, *Chron. D.S.*, 2004, p. 197.

¹⁰⁷ Pour d'autres décisions procédant à une analyse de la légalité d'un contrôle au regard de l'article 8 de la C.E.D.H., voy. : C.T. Bruxelles, 14 décembre 2004, *Computerr.*, 2005, p. 313 ; C.T. Bruxelles, 22 novembre 2005, *J.T.*, 2006, p.218.

¹⁰⁸ C.T. Liège, 20 mars 2006, *R.R.D.*, 2006, p. 89-101, note K. ROSIER et S. GILSON.

¹⁰⁹ C.T. Bruxelles (4^{ème} ch.), 28 novembre 2006, *Chr D.S.*, 2009, p. 32. Comp. : Trib. trav. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be.

¹¹⁰ T.T. Bruxelles (24^{ème} ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179 Comp. : Gand (12^{ème} ch., réf.), 16 juin 2004, *Chron. D.S.*, 2005, p. 48

¹¹¹ T.T. Liège (3^{ème} ch.), 3 septembre 2008, RG 371.015, www.cass.be; T.T. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be. Voyez également la décision du Tribunal du travail de Gand du 1^{er} septembre 2008 au sein de laquelle le Tribunal suggère que lorsque le contrôle porte sur des *e-mails* professionnels, il appartiendrait au travail de prouver en quoi son droit au respect de la vie privée serait violé (T.T. Gand, 1^{er} septembre 2008, RG 17054/06, www.cass.be).

¹¹² Voy. notamment à cet égard : K. ROSIER, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, 2009, n°35, pp. 126-140.

il faut s'en référer à la loi du 10 avril 1990 réglementant la sécurité privée et particulière qui prévoit, quant à elle, la possibilité d'effectuer également un contrôle d'entrée. Les conditions de ces textes sont nombreuses. Le contrôle doit, en tout cas, être exercé par un agent de gardiennage.

Les autres hypothèses de fouille (hors donc entrée et sortie) ne sont pas réglementées. La jurisprudence a dégagé des principes aux termes desquels la fouille peut s'avérer régulière moyennant le respect de certaines conditions. La Cour du travail de Liège¹¹⁴ a ainsi constaté que « *si la fouille d'un travailleur ou des biens de ce travailleur est considérée comme légitime dans certaines situations (cf. F. Lagasse, " La vie privée et le droit du travail ", Chr.D.S. 1997, 417, sp. p. 427 ; F. Lagasse et M. Milde, " Protection de la personne et vie privée du travailleur : investigation et contrôle sur les lieux de travail ", Orient. 1992, 149, sp. p.154, point 5), comme notamment pour vérifier qu'un vol n'est pas commis, il n'empêche que cette mesure constitue une atteinte inadmissible à la vie privée lorsqu'elle est effectuée sans l'accord de l'intéressé (accord qui peut résulter d'une disposition du règlement de travail) et au surplus, en son absence par une personne qui n'est pas dûment habilitée à ce faire* ». Elle précisait qu'« *en l'absence de règlement de travail envisageant la fouille des biens du membre du personnel, les employées qui avaient des soupçons auraient dû soit obtenir l'accord de l'intimée pour procéder à la fouille en sa présence, soit faire appel à la force publique pour éviter toute contestation quant à la régularité de la fouille ; qu'en s'investissant de pouvoirs dont elles ne disposaient pas, les employées et plus particulièrement Mme V. ont outrepassé leurs droits, empêchant par là de reconnaître toute validité aux constatations effectuées* ». Se dégage donc de cette disposition l'exigence du consentement du travailleur. On retrouve l'absence du consentement comme fondement au rejet des ainsi preuves obtenues dans d'autres décisions¹¹⁵.

Par ailleurs, la jurisprudence considère que le consentement de la travailleuse rend tout à fait licite la fouille. Ainsi, la Cour du travail de Mons a considéré qu'en donnant son consentement tacite aux demandes de fouille d'un gardien, la travailleuse a levé toute irrégularité éventuelle commise par celui-ci du fait du non respect de la loi du 10 avril 1990 réglementant la sécurité privée et particulière. Ces irrégularités résultaient de ce que ladite loi n'autorise ni l'interpellation de personnes, ni le contrôle du contenu de leur sac, ni leur interrogatoire et de ce que l'article 8, § 6 de la loi n'autorise le contrôle des vêtements et bagages « qu'à l'entrée dans un lieu gardé ». ¹¹⁶

38. Contrôle d'alcool et de drogues (C.C.T. 100)¹¹⁷ - La validité des tests d'alcoolémie devra désormais (à partir du 1^{er} avril 2010) être appréciée à l'aune de la nouvelle C.C.T. 100. De nombreuses difficultés pour concilier ce texte et d'autres normes légales ont déjà été relevées.

¹¹³ KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XI^{ème} colloque de l'association famille et droit, UCL, 30 novembre 2007, pp.6 et s.

¹¹⁴ C.T. Liège, 21 mai 2001, R.G. N°28.039/99, www.cass.be.

¹¹⁵ T.T. Nivelles (1^{ère} ch.), 8 février 2002, *J.T.T.*, 2002, p. 181 ; C.T. Bruxelles, 5 octobre 2004, R.G. n°42977, www.cass.be

¹¹⁶ C.T. Mons, 1^{ère} ch., 19 septembre 2003, *J.T.T.*, 2004, p. 197.

¹¹⁷ Voyez à ce sujet not. : W. VAN EECKHOUTTE et I. PLETS, « Alcohol en drugs op de arbeidsplaats : een zichtbaar taboe ? », *Chron. D.S.*, 2000, 569-584 et L. DEJAEGER, I. PLETS et W. VAN EECKHOUTTE, *Juridische handvaten voor het (problematisch) gebruik van alcohol en andere drugs op het werk*, Bruxelles, VAD, 2005, 120 p. Sur la C.C.T. C.C.T. 100, voyez : S.GILSON, *L'alcool et les drogues dans l'entreprise*, Vanden Broele, 2009 et les références citées.

39. Géolocalisation¹¹⁸ - Non spécifiquement réglementée¹¹⁹, la matière donne lieu à quelques décisions. La Cour du travail de Bruxelles, dans un arrêt du 18 novembre 2004¹²⁰, estime qu'en vertu des articles 16 et 17 de la loi du 3 juillet 1978 et de l'existence du lien de subordination sous lequel le travailleur effectue son travail, l'entreprise doit être à même d'exercer un contrôle sur le travailleur et que l'utilisation d'un GPS pour localiser les taxis ne constituerait pas une atteinte à la vie privée du chauffeur puisqu'il ne s'agit pas de l'espionner... Dans le même sens, le Tribunal du travail de Liège estime que, dès lors que le travailleur savait que l'enregistrement de données GPS le concernant était possible et que cet enregistrement a été réalisé pour contrôler l'emploi du temps du travailleur pendant son travail, le recours à cet enregistrement répond aux conditions de finalité et de proportionnalité et ne constitue pas une violation de la vie privée du travailleur¹²¹.

40. Usage du téléphone - Plusieurs décisions ont admis la production de factures destinées à établir l'existence d'appels passés à des fins privées sur un téléphone de l'entreprise en considérant que l'employeur pouvait produire les listings d'appels fournis par son opérateur de téléphonie¹²². La base légale serait, à nouveau, les articles 16 et 17 de la loi sur le contrat de travail du 3 juillet 1978. Il y avait eu une information préalable.

41. Documents stockés sur disque dur. Le sort des documents sauvegardés sur un PC mis à disposition du travailleur est controversé. Il a déjà été jugé qu'ils ressortaient à la vie privée du travailleur¹²³ (*« le fait que l'ordinateur sur lequel se trouvaient les documents est la propriété de la société n'exclut pas la protection qui s'attache au caractère personnel et privé des documents »*)., tout comme il a déjà été considéré que de tels fichiers ne peuvent revendiquer aucune protection¹²⁴. Sont visés ici des documents personnels du travailleur et non pas des documents de l'entreprise qu'il devrait utiliser, qui ne relèvent pas de la vie privée¹²⁵.

42. Correspondance¹²⁶. Dans un arrêt du 23 mars 2003, la Cour du travail de Liège a défini la correspondance comme un *« échange épistolaire confié à la poste ou à un organisme chargé de la distribution du courrier »*. Elle souligne que le principe de l'inviolabilité des lettres sanctionné à l'article 29 de la Constitution et 460 du Code pénal vaut à l'égard des autorités publiques mais qu'une fois la lettre remise à destination, ce sont les principes du droit privé qui garantissent le secret des correspondances vis-à-vis des citoyens entre eux. Dans ce cadre, la lettre en tant que message écrit adressé par une personne à une autre en vue de lui faire une communication (qui vise donc également les courriers remis en mains propres

¹¹⁸ MESSLIAEN, T., "Navigatiesystemen en privacy", *NJW*, 2007, 338-347; RENETTE, S. et DE BOT, D., « Het aanwenden van een geolocalisatiesysteem in het kader van een arbeidsovereenkomst », *Orientations*, 2005, 205-216.

¹¹⁹ La loi du 8 décembre 1992 trouve toutefois à s'appliquer (voy. K. ROSIER, « Preuve et données de géolocalisation, le point », n°380, p.5).

¹²⁰ C.T. Bruxelles (2^{ème} ch.), 18 novembre 2004, *J.T.*, 2005, p. 145.

¹²¹ T.T. Liège (5^{ème} ch.), 16 mai 2007, RG 358.538, www.cass.be.

¹²² T.T. Bruxelles (3^{ème} ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61; C.T. Liège, 21 mai 2001, *J.T.T.*, 2002, p. 180; C.T. Gand, 22 octobre 2001, *J.T.T.*, 2002, p. 41.

¹²³ C.T. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262.

¹²⁴ C.T. Liège (sect. Namur), 11 janvier 2007, *R.R.D.*, 2007, p. 488, note K. ROSIER et S. GILSON ; *J.T.T.*, 2007, p. 249.

¹²⁵ Gand, 6 janvier 2004, *T.G.R.*, 2004, p. 56.

¹²⁶ Voyez à cet égard, R. ROBERT, « Correspondance et vie privée sur les lieux de travail : une cohabitation difficile », *Orientations*, 2008, n°7, pp. 16-22

à un destinataire ou déposés à son intention) est protégée mais sur la base, non du principe de l'inviolabilité des lettres, mais sur celle des principes de droit privé liés au respect de la vie privée¹²⁷. La Cour du travail de Liège, dans un arrêt du 25 avril 2002, a appliqué cette même exigence de respect de la vie privée à l'égard d'un carnet destiné à consigner les observations confidentielles d'un patient et de sont psychologue¹²⁸. La Cour avait considéré que le respect de la vie privée englobait tout écrit confidentiel, même si le carnet en question ne pouvait être qualifié de correspondance au sens de l'article 29 de la Constitution et de l'article 460 du Code pénal. La protection de la correspondance s'adresse cependant aux courriers confidentiels et non aux courriers d'entreprise. Il appartient au Juge de déterminer si un courrier est ou non confidentiel¹²⁹.

La question de la production d'une lettre ou missive qui pourrait enfreindre le respect de la vie privée par un tiers qui n'est ni l'auteur, ni le signataire est délicate. On rencontre des décisions qui divergent sur les conditions dans lesquelles un tel document peut être produit. Ainsi selon une certaine jurisprudence, si le tiers s'est procuré régulièrement la lettre, il est admis qu'il puisse la produire¹³⁰. D'autres décisions recensées estiment qu'une correspondance qui serait confidentielle doit être rejetée des débats à moins qu'elle ne soit produite avec l'accord de son auteur¹³¹.

43. Détective - Le recours à un détective privé, dans le cadre de la relation de travail, est de plus en plus fréquent. La reconnaissance de profession de détective par la loi du 19 juillet 1991 a entraîné une certaine évolution de la jurisprudence vers une admission prudente, parce qu'il s'agit tout de même d'une personne payée par une partie au litige, des constatations du détective. Au regard de l'article 8 de la convention européenne des droits de l'homme, si les conditions de légalité et de légitimité paraissent réunies¹³², la condition de proportionnalité est sans doute la plus délicate. Il est en tout cas clair que l'intervention du détective privé doit respecter strictement les critères de la loi du 19 juillet 1991 qui prévoit, notamment, l'interdiction d'observer des personnes dans des lieux non accessibles au public ou encore l'interdiction de recueillir des données sensibles. Il y a lieu également d'apprécier l'intervention du détective privé au regard de la loi du 8 décembre 1992, ce qui est susceptible de poser certaines difficultés en ce qui concerne les obligations qui pèsent sur le responsable du traitement et, notamment, l'obligation d'information de la personne concernée¹³³.

¹²⁷ C.T. Liège, 23 mars 2004, *R.R.D.*, 2004, p. 73.

¹²⁸ C.T. Liège, 25 avril 2002, *J.L.M.B.*, 2003, p. 107, *R.R.D.* 2002, p. 266, note F. LAGASSE.

¹²⁹ H. BUYSENS, *op. cit.*, 1999, p. 17.

¹³⁰ C.T. Liège, 23 mars 2004, *R.R.D.*, 2004, p. 73 ; voyez aussi N. VERHEYDEN-JEANMART, *op.cit.*, p. 292.

¹³¹ C.T. Liège, 23 mars 2004, *R.R.D.*, 2004, p. 73 ; C.T. Liège, 25 avril 2002, *J.L.M.B.*, 2003, p. 107; *R.R.D.*, 2002, p. 266, note F. LAGASSE : la Cour du travail de Liège avait dès lors rejeté le carnet confidentiel comme preuve même si l'employeur n'avait commis aucune faute en le réceptionnant.

¹³² Voyez l'arrêt VERLIERE du 28 juillet 2001, précité.

¹³³ Sur cette question, on lira avec intérêt l'étude de D. MOUGENOT, « Humphrey Bogaert au 21^{ème} siècle : la preuve par production d'un rapport de détective privé », note sous C.T. Liège, 15 décembre 2008, *Revue régionale de droit*, 2009, p. 242 et s.

CHAPITRE V : LA VIE PRIVEE LORS DE LA SUSPENSION DU CONTRAT¹³⁴

44. La cause de suspension doit être justifiée. Le droit social a envisagé une série d'hypothèses dans lesquelles le travailleur peut solliciter la suspension de son contrat de travail avec ou sans maintien de sa rémunération, selon les cas. Le travailleur qui invoque la cause de suspension doit prouver l'événement qui justifie celle-ci. Ainsi, par exemple, pour les congés de circonstances liées à des événements familiaux, à des obligations civiles, etc., le travailleur aura l'obligation d'apporter la preuve, si l'employeur lui demande, des circonstances ayant justifié le congé ; par exemple, un certificat de décès du proche dans le cadre de certains congés de circonstances. Le travailleur doit également prouver l'utilisation conforme du congé pour raison impérieuse prévue par la C.C.T. n° 45 du 19 décembre 1989. La vie privée n'est donc pas absolue.

45. La protection des données relatives à l'état de santé du travailleur. La situation la plus fréquente, et sans doute la plus sensible, est l'incapacité de travail par suite de maladie ou d'accident. Le législateur est alors intervenu pour concilier la nécessité pour l'employeur d'obtenir une preuve de la cause de la suspension, d'autant que celle-ci va entraîner le paiement d'un salaire garanti et la vie privée du travailleur¹³⁵. Le législateur va ainsi prévoir que l'obligation de justification du travailleur se fait par un certificat médical qui mentionne l'incapacité de travail, sa durée probable et si le travailleur peut ou non se rendre à un autre lieu pour le contrôle. Il n'est donc jamais question de la nature de l'affection (art. 31, § 2, alinéas 2 et 3). L'article 31, § 3 de la loi du 3 juillet 1978 régit également strictement le contrôle par l'employeur de l'incapacité en le réservant à un médecin contrôleur dont la mission est entourée de certaines garanties et en limitant le contrôle des informations récoltées à la vérification de la réalité de l'incapacité de travail et de sa durée¹³⁶.

CHAPITRE VI : LA VIE PRIVEE LORS DE LA RUPTURE DU CONTRAT¹³⁷

1. PRÉLIMINAIRES : MOTIVATION ET MOTIFS DU CONGE

46. Absence d'obligation générale de motivation du congé. Le droit belge ne comporte pas, en règle, *d'obligation générale de motivation formelle* du congé, sauf quelques exceptions notables (licenciement pour motif grave, licenciement de certains représentants des travailleurs, licenciement des contractuels de la fonction publique¹³⁸. L'employeur n'a donc

¹³⁴ Sur cette question, voyez not. : N. HAUTENNE, K. ROSIER et S. GILSON, « Les informations médicales dans la relation de travail », *Orientations*, 2005, numéro spécial, 61-95.

¹³⁵ Sur cette question, voyez not. : DAVAGLE, M., *L'incapacité de travail de droit commun et les obligations qui en découlent pour l'employeur et le travailleur*, Kluwer, 2006, p. 328 ; HAUTENNE, N., ROSIER, K. et GILSON, S., « Les informations médicales dans la relation de travail », *Orientations*, 2005, numéro spécial, 61-95.

¹³⁶ BEAUFILS, N., « La loi du 13 juin 1999 sur la médecine de contrôle et ses implications sur le contrôle de l'incapacité de travail », *J.T.T.*, 2001, 73-78 ; KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XIème colloque de l'association famille et droit, UCL, 30 novembre 2007, p.13

¹³⁷ C. WANTIEZ, « La rupture du contrat de travail », in *Vie privée du travailleur et prérogatives patronales*, Ed. du Jeune Barreau de Bruxelles, 2005, p. 215.

¹³⁸ S. GILSON, « L'absence de motivation formelle du congé, une règle en sursis ? L'exemple du licenciement des contractuels de la fonction publique », *Orientations*, n° 4, avril 2006, pp. 8 et svtes ; S.GILSON, contribution

pas l'obligation de faire part, dans la lettre de congé, des motifs du licenciement intervenu. Par ailleurs, sauf dans certains cas plus rares encore (licenciement de certains représentants des travailleurs), il n'y a pas de procédure d'autorisation *a priori* du licenciement, qu'elle soit administrative ou judiciaire.

47. Contrôle des motifs du licenciement. Dans toute une série d'hypothèses, des faits de la vie privée se voient protéger et ne peuvent être érigés en motif de licenciement. Il en va ainsi pour l'usage d'un certain nombre de droits mais également, par exemple, pour la maternité : congé parental, crédit-temps, etc. Dans ces hypothèses, le travailleur bénéficie le plus souvent de « protections contre le licenciement ». L'incidence de « protection contre le licenciement » sera également d'obliger l'employeur à justifier *a posteriori* le congé et à prouver qu'il est étranger à la cause de protection. Ce faisant, la circonstance de vie privée protégée ne peut être un motif de licenciement¹³⁹.

En dehors de ces hypothèses de protection contre le licenciement, et hors motif grave, l'employeur décide seul, pour des motifs qu'il ne doit pas communiquer dans la lettre de congé, du licenciement des travailleurs. Contrairement à ce qui est soutenu bien souvent, cela n'en rend pas son droit de licencier *discrétionnaire*. Celui-ci doit, en effet, s'exercer dans le respect de certains principes dont on retiendra d'ores et déjà le principe de non-discrimination¹⁴⁰ ou encore l'interdiction de l'abus de droit. En matière contractuelle, la Cour de cassation se base sur l'article 1134 du Code civil pour fonder l'abus de droit, en application du principe d'exécution de bonne foi des conventions¹⁴¹. L'examen de l'abus de droit variera selon que le travailleur est un ouvrier et peut bénéficier de la disposition protectrice de l'article 63 de la loi du 3 juillet 1978 ou un employé qui doit apporter la preuve d'une faute de l'employeur.

2. FAITS DE LA VIE PRIVÉE COMME MOTIFS DU CONGÉ

48. Licenciement pour motif grave. Les faits de la vie privée ne bénéficient pas, en tant que tels, parce qu'ils ressortent de la vie privée, d'une sphère d'immunité. Dans le cas du licenciement pour motif grave, il est admis que la faute ne doit pas être une faute nécessairement contractuelle¹⁴², il peut donc s'agir d'un acte de la vie privée¹⁴³. Ce qui compte d'une certaine façon c'est de savoir si ces faits de la vie privée sont fautifs et sont de nature à rendre définitivement et immédiatement impossible la poursuite des relations contractuelles. Il peut ainsi être admis qu'un employeur soit ébranlé par le fait d'apprendre

à l'après-midi d'étude de l'UCL, *Motivation et motifs du congé*, « Le congé notifié à un agent contractuel de la fonction publique et l'irruption de la loi du 29 juillet 1991 : une véritable exception à la règle d'absence de motivation du congé en droit social » in *La motivation du congé*, Kluwer 2006)

¹³⁹ KEFER, F. et MAISETTI, P., « La vie personnelle du salarié » in *Les droits de la personnalité*, Documents du XI^{ème} colloque de l'association famille et droit, UCL, 30 novembre 2007, p.24

¹⁴⁰ La loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination¹⁴⁰, qui a transposé la Directive 2000/78/CE du Conseil du 27 novembre 2000 portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail a abrogé les articles 2 à 11 de la loi du 13 février 1998 portant des dispositions en faveur de l'emploi. La loi a créé un cadre général pour lutter contre la discrimination fondée sur les critères suivants : l'âge, l'orientation sexuelle, l'état civil, la naissance, la fortune, la conviction religieuse ou philosophique, la conviction politique, la langue, l'état de santé actuel ou futur, un handicap, une caractéristique physique ou génétique ou l'origine sociale (art. 3 de la loi).

¹⁴¹ Cass., 19 septembre 1983, *R.C.J.B.*, 1986, p. 282.

¹⁴² Cass., 6 mars 1995, *J.T.T.*, 1995, p. 281, note Claude WANTIEZ.

¹⁴³ Cass., 9 mars 1987, *J.T.T.*, 1987, p. 128.

que son travailleur vole dans sa vie privée et que c'est de nature à rompre la confiance¹⁴⁴. La simple condamnation du travailleur, même pour des raisons qui sont sans lien avec l'exécution du contrat de travail, est souvent jugée suffisante¹⁴⁵.

49. Applications - L'examen des motifs graves s'apparente, bien souvent, à une casuistique. Il est difficile d'en tirer des lignes directrices¹⁴⁶ tant les situations varient. Tel fait peut être considéré comme fautif mais non suffisant que pour justifier un motif grave dans le cas d'espèce.

Il a été jugé que l'usage de *stupéfiants*, même à titre privé, pouvait être un motif grave de licenciement pour une vendeuse en contact direct avec la clientèle et responsable de la recette journalière¹⁴⁷. Une jurisprudence abondante a trait à l'alcoolisme.

Plus délicates encore sont les questions des *relations amoureuses* qui se développent entre les membres du personnel. Ont déjà été considérés comme motifs graves une liaison adultère entre travailleurs ayant un lien hiérarchique¹⁴⁸, une relation amoureuse avec une subordonnée¹⁴⁹, une relation amoureuse avec une patiente¹⁵⁰, l'entretien de relations sexuelles avec un des membres du personnel à l'intérieur des bâtiments¹⁵¹. A condition toutefois, selon nous, que cela puisse susciter critique, par exemple par une influence négative au sein de l'entreprise, un favoritisme, l'impossibilité d'exercer l'autorité, etc¹⁵².

La jurisprudence semble admettre que le *droit du travailleur de se vêtir comme il le souhaite* peut être influencé par la nature de sa fonction et de l'entreprise dans laquelle il exerce, de sorte que n'ont pas été jugés abusifs des licenciements fondés sur une tenue qui ne cadrerait pas avec les pratiques de l'entreprise¹⁵³. La jurisprudence tient toujours compte des circonstances, rejetant ainsi le motif grave issu du fait qu'une personne transsexuelle ayant subi une opération décide de se vêtir en femme¹⁵⁴.

50. Licenciement moyennant préavis ou indemnités. Si un fait de la vie privée peut justifier un motif grave, *a fortiori* pourrait-il être la cause d'un licenciement moyennant préavis ou indemnités. La question cruciale reste identique : le fait de la vie privée est-il susceptible de justifier le licenciement envisagé comme un droit-fonction devant être exercé par l'employeur dans une finalité socio-économique. Il est donc question de l'incidence sur le travail du fait de la vie privée.

51. Caractère abusif du licenciement fondé sur un fait de la vie privée ? Dans le régime des ouvriers l'employeur doit prouver un motif en lien avec l'attitude (fut-elle non fautive),

¹⁴⁴ C.T. Liège, 27 juin 1975, *Bull. F.E.B.*, 1977, p. 1958.

¹⁴⁵ C.T. Liège, 13 septembre 2006, *J.T.T.*, 2007, p. 60.

¹⁴⁶ Voyez à ce sujet, B.PATERNOSTRE, *Motif grave : les enseignements de la jurisprudence*, Kluwer, 2008.

¹⁴⁷ C.T. Liège, 21 juin 1995, *J.T.T.*, 1996, p. 145.

¹⁴⁸ C.T. Mons, 28 novembre 1977, *J.T.T.*, 1978, p. 6.

¹⁴⁹ C.T. Gand, 26 juin 1991, *Bull. F.E.B.*, 1994/12, p. 71.

¹⁵⁰ C.T. Liège, 14 mars 2002, *J.L.M.B.*, 2003, p. 107.

¹⁵¹ C.T. Gand, 4 mars 1992, *J.T.T.*, 1993, p. 55.

¹⁵² cf. Trib. trav. Bruxelles, 4 novembre 1991, *R.W.*, 1991-1992, p. 784 ; C.T. Mons, 28 novembre 1977, *J.T.T.*, 1978, p. 6.

¹⁵³ Voyez ainsi C.T. Bruxelles, 10 juillet 1992, *Chron. D.S.*, 1993, p. 89 et C.T. Mons, 6 septembre 1985, inédit R.G. : 15.970 cité in C.E. CLESSE, *Le licenciement abusif*, Kluwer, 2005, p. 88 et 89.

¹⁵⁴ Trib. trav. Bruxelles, 10 octobre 1994, *R.D.S.*, 1994, 349 ; note F. HENDRICKX, « Het recht op privacy van de transeksuele werknemer bij het ontslag om dringende reden », *R.D.S.*, 1994, 343-347.

l'aptitude ou les nécessités économiques. Il n'est donc pas exclu que des faits de la vie privée, qui auraient trait à l'attitude du travailleur, et qui ne se verraient pas par ailleurs protégés (hypothèse notamment des protections contre le licenciement), puissent rendre le congé non abusif. Dans le régime des employés, le travailleur se trouvera bien souvent confronté à la difficulté d'apporter la preuve d'une faute de l'employeur. Dans tous les cas, à notre sens, c'est la finalité du congé qui doit être interrogée : le congé peut-il se justifier à l'aune de l'intérêt légitime de l'entreprise ? C'est donc toujours la répercussion du fait de vie privée sur le travail qui pourrait constituer le motif du congé et non le fait de vie privée en tant que tel. La problématique se révèle de manière très nette dans le congé fondé sur l'état de santé, situation personnelle touchant à la vie privée¹⁵⁵.

52. Méconnaissance par le travailleur de la vie privée. On peut imaginer les hypothèses où l'infraction à des règles de protection de la vie privée par le travailleur puisse constituer elle-même un motif de licenciement. La jurisprudence a ainsi eût à connaître du cas de travailleurs consultant irrégulièrement, dans le cadre de leurs fonctions, le registre national. Le comportement, en toute hypothèse fautif, a donné lieu, selon les circonstances, à l'admission du motif grave ou, au contraire, à son rejet.

53. Violation de la vie privée par l'employeur par la publicité donnée au licenciement. L'employeur peut également méconnaître la vie privée du travailleur dans les modalités de licenciement, notamment en donnant une publicité abusive à celui-ci¹⁵⁶ ce qui peut justifier le caractère abusif de celui-ci.

54. Violation de la vie privée par l'employeur dans la collecte de la preuve des motifs du congé. Nous aborderons ce point *infra*.

CHAPITRE VII : LES SANCTIONS DE LA VIOLATION DE LA VIE PRIVEE

1. ABSENCE DE MODES DE RÉPARATION SPÉCIFIQUES – MISE EN CAUSE DE LA RESPONSABILITÉ CIVILE.

55. Sanctions pénales – sanctions civiles. Un certain nombre de dispositions protectrices de la vie privée sont sanctionnées pénalement. Il en va ainsi également pour les conventions collectives de travail rendues obligatoires par arrêté royal. Force est de constater, pourtant, que la mise en œuvre de sanctions pénales dans ce cadre est rare. Il n'y a, en règle générale, pas de sanction spécifique qui soit attachée à la violation de la vie privée, de sorte que l'on recourt à la responsabilité civile, souvent contractuelle lorsqu'il s'agit, par exemple, d'une violation dans la collecte des modes de preuves liés à un congé. La violation de la vie privée est souvent abordée sous l'angle du caractère abusif du congé mais elle pourrait très bien en être dissociée.

¹⁵⁵ S. GILSON et A. ROGER, « Etat de santé et licenciement abusif », in *Le licenciement abusif. Notion, évolution, perspectives*, C.E. CLESSE et S. GILSON, dir., Anthemis 2009

¹⁵⁶ Voyez les exemples cités in C.E. CLESSE, *Le licenciement abusif*, Kluwer, 2005, p. 135 et 136.

2. IRRECEVABILITÉ DE LA PREUVE¹⁵⁷

56. L'écartement de la preuve irrégulièrement acquise. La règle de base qui était admise était, en matière civile, le principe de l'exclusion des preuves illégales et irrégulières¹⁵⁸. La Cour de cassation avait toutefois déjà assoupli sensiblement sa jurisprudence en matière pénale¹⁵⁹.

57. Les arrêts *Antigone* et *Manon*. Dans son arrêt « *Antigoon* » du 14 octobre 2003¹⁶⁰, la Cour de cassation admet qu'il puisse y avoir égard à des preuves recueillies illicitement sauf exceptions définies par la Cour : lorsque le respect de certaines conditions de forme est légalement prescrit à peine de nullité ; lorsque l'irrégularité commise entache la crédibilité de la preuve ; lorsque l'usage de cette preuve est contraire au droit à un procès équitable. Un autre arrêt du 2 mars 2005, rendu en matière pénale mais dans un contexte de relation de travail (obtention d'une preuve en violation de l'information préalable requise par l'article 9 de la C.C.T. n°68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail)¹⁶¹ estime également que le Juge peut, pour fonder l'admission des éléments irrégulièrement produits, prendre en considération notamment la circonstance que l'illicéité est sans commune mesure avec la gravité de l'infraction dont l'acte irrégulier a permis la constatation ou que cette irrégularité est sans incidence sur le droit ou la liberté protégés par la norme transgressée.

58. L'application de la jurisprudence *Antigone* et *Manon* aux litiges civils¹⁶². Dans un premier temps, les juges du fond ont estimé cette jurisprudence inapplicable en matière civile¹⁶³. Un arrêt du 10 mars 2008 de la Cour de cassation¹⁶⁴, rendu cette fois en matière civile dans un litige de chômage, repose la question. La Cour y étend sa jurisprudence à la

¹⁵⁷ S. GILSON et K. ROSIER « La preuve en droit du travail », *Orientations*, avril 2007, pp. 1 à 17 ; S. GILSON, K. ROSIER et E. DERMINE, « La preuve en droit social », in *La preuve, questions spéciales*, CUP, F. KUTY et D. MOUGENOT (dir.), Anthémis, 2008, pp. 179 et s. ; K. ROSIER et S. GILSON, « Licéité de la preuve et droit au respect de la vie privée : principes et sanctions : note sous Cour. trav. Mons (2e ch.), 18 février 2008 et Cour trav. Mons (3e ch.), 22 mai 2007 », *R.D.T.I.*, 2008, n° 31, pp. 229-258 ; K. ROSIER et S. GILSON, « Non-respect de la vie privée du travailleur dans le recueil de la preuve du motif grave : quand l'abusé devient abuseur... », *R.R.D.*, 2007, pp. 498-508 ; K. ROSIER et Th. LEONARD, « La jurisprudence "Antigoon" face à la protection des données : salvatrice ou dangereuse ? », *R.D.T.I.*, 2009, n° 36, pp. 5-10.

¹⁵⁸ F. KUTY, « Le droit de la preuve à l'épreuve des juges », *J.T.*, 2005, p. 349.

¹⁵⁹ Cass., 17 janvier 1990, N° 7831, www.cass.be ; en ce sens, Cass., 17 avril 1991, N° 8761, www.cass.be ; Cass., 30 mai 2005, *Pas.*, 1995, p. 566. ; Cass. (2^{ème} ch), 27 février 2001, *R.G.A.R.*, 2002, p. 13605 ; Cass., 23 mars 2004, N° P.04.0012.N, www.cass.be.

¹⁶⁰ Cass., 14 octobre 2003, N° P.03.0762.N, www.cass.be, avec les conclusions de l'avocat général De Swaef.

¹⁶¹ Cass., 2 mars 2005, *J.T.*, 2005, p.211, conclusions de l'avocat général D. VANDERMEERSCH, *J.L.M.B.*, 2005, p.1086, note M.-A. BEERNAERT.

¹⁶² Sur cette question voy. F. HENDRICKX, "Privacy op het werk en bewijs van onrechtmatig gedrag : (spook) Antigoon in het arbeidsrecht?", *R.D.S.*, 2006, 659-704 ; I. VERHELST et N. THOELLEN, "Over privacy, controle en (on)rechtmatig verkregen bewijs", *Or.*, 2008, 8, 197-208 ; F.KEFER, "Antigone et Manon s'invitent en droit social. Quelques propos sur la légalité de la preuve », *R.C.J.B.*, 2009, p.333

¹⁶³ T.T. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be ; T.T. Liège (3^{ème} ch.), 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. ROSIER et S. GILSON ; *J.L.M.B.*, 2008, p. 389 ; C.T. Bruxelles (4^{ème} ch.), 9 janvier 2007, RG 45.657, *inédit* ; T.T. Bruxelles (3^{ème} ch.), 16 mars 2006, *inédit* cité par F. GILLET, « Une preuve obtenue en violation des dispositions de la C.C.T. n°68 est illicite, de même que l'aveu obtenu sur cette base », www.hrttoday.be. Pour une application de la jurisprudence de la Cour de cassation dans un litige civil, voyez cependant l'arrêt rendu par la Cour d'appel de Mons le 2 mai 2005 (Mons, (1^{ère} ch.), 2 mai 2005, *J.L.M.B.*, 2005, p. 438).

¹⁶⁴ Cass., 10 mars 2008, *Or.*, 2008, p.172, note I. PLETS ; *J.L.M.B.*, 2009, p.580, note R. DEBAERDEMAEKER.

matière civile. Il s'agissait toutefois d'un litige portant sur une sanction administrative dont on pourrait soutenir qu'elle a une nature pénale au sens de la jurisprudence de la Cour européenne des droits de l'homme¹⁶⁵. La jurisprudence *Antigone* semble se développer en droit social après une réticence des juges du fond. Ainsi, un arrêt de la Cour du travail d'Anvers rendue le 2 septembre 2008¹⁶⁶ avait à se prononcer sur la validité d'un contrôle opéré par un le responsable du département ICT de l'entreprise qui avait révélé qu'un employé avait utilisé une connexion réservée au serveur *mail* de l'entreprise pour ses communications personnelles -et ce vraisemblablement dans le but de se soustraire au système de contrôle de l'usage de l'internet et de l'*e-mail* mis en place par l'employeur-. Au terme d'une analyse pointilleuse de la régularité du contrôle au regard du cadre réglementaire applicable, la Cour est confrontée à la question du respect de l'obligation d'informer le travailleur. Elle accepte cependant de tenir compte des éléments de preuve produits et indiquant que, à supposer même qu'il y ait eu une irrégularité dans la procédure d'information, celle-ci n'entacherait pas la fiabilité de la preuve ni ne priverait le travailleur d'un procès équitable, faisant ainsi application de la jurisprudence « *Antigoon* ».

58. L'arrêt *Davies* de la C.E.D.H.¹⁶⁷. La jurisprudence de la Cour européenne des droits de l'homme ne semble pas s'opposer à une telle lecture. Ainsi, dans un arrêt du 28 juillet 2009, la Cour Européenne des Droits de l'Homme eut l'occasion de se prononcer sur la validité, au regard de l'article 6 de la C.E.D.H., de la jurisprudence *Antigone* de la Cour de cassation¹⁶⁸. La Cour rappelle, tout d'abord, que ledit article 6 ne régit pas l'admissibilité des preuves en tant que telle de sorte que cette matière doit être réglée par le droit interne et qu'il ne lui appartient pas de se prononcer sur le principe de l'admissibilité des preuves recueillies illégalement. En revanche, il lui revient d'examiner si la procédure a été équitable, et ce dans son ensemble. Il en résulte que son examen peut à ce titre porter également sur la manière dont les éléments de preuve ont été recueillis et sur l'illégalité en cause, qu'elle concerne le droit interne et/ou une disposition de la C.E.D.H.. Il pourrait être considéré que les enseignements de cet arrêt viennent conforter la jurisprudence de la Cour de cassation qui se fondait d'ailleurs notamment sur la considération selon laquelle l'article 6 C.E.D.H. n'impliquait pas qu'une preuve qui a été obtenue en méconnaissance d'un droit fondamental garanti par la Convention précitée ou par la Constitution, n'est jamais admissible¹⁶⁹. A notre sens toutefois, et comme la Cour le rappelle, la C.E.D.H. ne règle pas la matière de l'admissibilité de la preuve et, si elle n'est pas un obstacle à la jurisprudence de la Cour de cassation, ne modifie pas le régime antérieur de légalité des preuves qui était certes issu uniquement de la jurisprudence et de la doctrine.

59. Le sort des autres preuves recueillies sur base d'une preuve irrégulière. La jurisprudence considère majoritairement que les aveux obtenus à la suite de moyens de preuves illégaux doivent être considérés eux-mêmes comme illégaux¹⁷⁰. Cette question subira sans doute les mêmes discussions que celles liées à la recevabilité de la preuve.

¹⁶⁵ Voyez en ce sens : C.T. Liège, 22 janvier 2008, RG n° 7968/05 ; C.T. Liège, 18 décembre 2008, RG n° 35.467/08 ; M. DELANGE, « Les mesures d'exclusion en matière de chômage après l'arrêt royal du 29 juin 2000 sur la réforme des sanctions administratives », *Chron. D. S.*, 2002, en particulier, p. 485.

¹⁶⁶ C.T. Anvers (sect. Hasselt), 2 septembre 2008, *Orientations*, 2009, p. 22, note K. ROSIER.

¹⁶⁷ K. ROSIER, « La Cour européenne des droits de l'homme confrontée à la jurisprudence *Antigone* », *Bulletin social et juridique*, 2010, n°423, p.6.

¹⁶⁸ Cour Eur. D. H., Arrêt *Lee Davis c. Belgique* du 28 juillet 2009, <http://www.echr.coe.int/echr/>.

¹⁶⁹ Cass, 16 novembre 2004, RG P041127N, www.cass.be.

¹⁷⁰ T.T. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be; T.T. Liège (3^{ème} ch.), 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. ROSIER et S. GILSON ; *J.L.M.B.*, 2008, p. 389; C.T. Bruxelles (2^{ème} ch.), 15 juin 2006, *J.T.*,

2. OCTROI DE DOMMAGES ET INTÉRÊTS

60. Des dommages et intérêts peuvent être octroyés pour violation de la vie privée . Dans un jugement du 6 mars 2007¹⁷¹, le Tribunal du travail de Liège a considéré que l'employeur, en obtenant des images de façon irrégulière, a manqué au principe de la loyauté dans le cadre de l'exécution de contrat de travail. Il condamne l'employeur à des dommages et intérêts en se fondant sur un manquement à l'article 16 de la loi sur le contrat de travail ainsi sur l'existence d'une faute au sens de l'article 1382 du Code civil. Ce faisant, le Tribunal épingle le recueil de la preuve par caméra de manière irrégulière comme constituant un comportement fautif réalisé au Cours du processus ayant abouti au licenciement. Il qualifie ce comportement de « faute dans l'exercice du droit de licencier au sens large ». Le Tribunal juge également que la travailleuse démontre avoir subi un dommage du fait de ce comportement fautif, dommage consistant en une atteinte à sa vie privée.

La Cour du travail de Liège avait également octroyé des dommages et intérêts en raison de la production de courriers électroniques dont l'employeur avait irrégulièrement pris connaissance¹⁷². La Cour considéra que la prise de connaissance irrégulière de courriers électroniques ainsi que le fait de les imprimer et de les produire en justice relèvent d'une défense en justice abusive et estime que l'écartement de cette pièce ne suffit pas à réparer le dommage et octroie à la travailleuse des dommages et intérêts.

2006, p. 492 ; C.T. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p.262 ; T.T. Bruxelles (3^{ème} ch.), 16 mars 2006, *inédit* cité par F. GILLET, « Une preuve obtenue en violation des dispositions de la C.C.T. n°68 est illicite, de même que l'aveu obtenu sur cette base », www.hrttoday.be; C.T. Bruxelles, 14 décembre 2004, *Computerr.*, 2005, p. 313 ; T.T. Nivelles (1^{ère} ch.), 8 février 2002, *J.T.T.*, 2002, p.181 ; T.T. Liège (3^{ème} ch.), 19 mars 2008, RG 360.454, www.cass.be.

¹⁷¹ T.T. Liège (3^{ème} ch.), 6 mars 2007, *R.R.D.*, 2007, p. 498, note K. ROSIER et S. GILSON ; *J.L.M.B.*, 2008, p. 389.

¹⁷² C.T. Liège (sect. Namur), 11 janvier 2007, *R.R.D.*, 2007, p. 488, note K. ROSIER et S. GILSON.

EXPÉRIENCES CONCRÈTES SUR LE LIEU DE TRAVAIL

Manu Gonzalez, Stephan Galon

Biographie sommaire

Manu Gonzalez est itinérant syndical dans une grande entreprise de la distribution sur la région bruxelloise et ce depuis plus de 20 ans pour la cne-csc.

Stephan Galon is directeur van het Internationaal Departement van ABVV.

Hij is ook stichtend lid van het Platform voor Vrije Meningsuiting en afgevaardigd beheerder van de vzw Belga-Vox. Hij zetelt tevens in de Raden van Beheer van FOS-Socialistische Solidariteit en Solidarité Socialiste.

PROCEDURES AND ACTIONS AGAINST LIDL, SIEMENS AND OTHER COMPANIES IN GERMANY

Dieter Hummel

*Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,*

in den vergangenen Wochen und Monaten ist es in der Bundesrepublik eine Vielzahl von Fällen bekannt geworden, in denen Arbeitgeber die Persönlichkeitsrechte der Arbeitnehmer verletzt haben. Eine kleine Auswahl:

Die Deutsche Bahn und die Telekom haben ihre Beschäftigten bespitzelt und teilweise deren Konten überprüfen lassen, Daimler Benz hat illegal Krankendaten über seine Beschäftigten gesammelt, Lidl und Schlecker, zwei große Einzelhandelsunternehmen, haben illegale Überwachungen ihrer Beschäftigten mit Hilfe von Videokameras durchgeführt, große Rundfunkunternehmen in der Bundesrepublik haben bei der Einstellung von Beschäftigten Blutscreenings durchgeführt.

Diese Fälle, die an die Öffentlichkeit gelangt sind, sind jedoch nur ein kleiner Teil des Missbrauchs von Arbeitnehmerdaten im betrieblichen Alltag in der Bundesrepublik Deutschland. Täglich werden, ohne dass dies groß an die Öffentlichkeit gelangt, in Warenhäusern Beschäftigten illegal durch Video überwacht, täglich werden E-Mails, die Beschäftigte verschicken, durch die Arbeitgeber mitgelesen, ohne dass es hierfür eine rechtliche Erlaubnis gibt, es werden illegale Datensammlungen hinsichtlich von Krankheiten und deren Diagnosen über Beschäftigte angelegt und es werden täglich, ohne dass es rechtlich zulässig wäre, z. B. in Callcentern Telefongespräche von Beschäftigten überwacht.

Darüber hinaus findet täglich auch eine legale Verletzung der Privatsphäre von Beschäftigten statt. Arbeitgebern ist es aufgrund betrieblicher Vereinbarungen erlaubt, eine fast vollständige Überwachung der Beschäftigten z. B. durch Video durchzuführen oder in Callcentern die Gespräche, die Beschäftigte mit dem Kunden führen, fast vollständig mitzuschneiden und personenbezogen auszuwerten sowie diese Erkenntnisse zur Grundlage von Leistungsbeurteilungen und Entlohnung zu machen.

Hierzu muss man wissen, dass es in der Bundesrepublik kein eigenes Gesetz zum Schutz von Arbeitnehmerdaten gibt. Der Schutz der Arbeitnehmerdaten soll über das allgemeine Gesetz zum Schutz privater Daten, das Bundesdatenschutzgesetz, gewährleistet werden. Dieses Gesetz sah über lange Zeit seines Bestehens einen Schutz, der besonders auf die Arbeitnehmer zugeschnitten war, kaum vor. Erst im Zuge der oben geschilderten Skandale wurde mit § 32 Bundesdatenschutzgesetz der Arbeitnehmerdatenschutz stärker in den Mittelpunkt gerückt, ohne dass dies jedoch ein ausreichender Schutz sein kann. Geregelt wurde lediglich in allgemeiner Art, dass eine Überwachung von Beschäftigten nur unter bestimmten Voraussetzungen zulässig sein

soll. Diese Voraussetzungen sind jedoch sehr allgemein und sehr weit geschaffen, so dass sie einen tatsächlichen Schutz der Beschäftigten nicht darstellen.

Darüber hinaus ist wichtig zu verstehen, dass in § 4 des Bundesdatenschutzgesetzes, diese Vorschrift regelt allgemein die Zulässigkeit der Datenerhebung, Verarbeitung und Nutzung, vorgesehen ist, dass eine Erhebung und Verarbeitung von Daten unter anderem dann zulässig ist, wenn eine Rechtsvorschrift dies vorsieht. In diesen Fällen ist eine Datenerhebung auch ohne Mitwirkung und Wissen des jeweiligen betroffenen Beschäftigten möglich. Eine solche Rechtsvorschrift sind Vereinbarungen zwischen den Betriebsräten und dem Arbeitgeber, so genannte Betriebsvereinbarungen. Betriebsvereinbarungen sind im deutschen Recht Regelungen zwischen dem Betriebsrat, also der Arbeitnehmervertretung, die im Betrieb gewählt ist und dem Arbeitgeber, die normativen Charakter haben, also für die Beschäftigten Regelungen treffen, die unmittelbar und zwingend sind. Nach § 4 Abs. 2 Nr. 1 Bundesdatenschutzgesetz können also solche Betriebsvereinbarungen mit unmittelbarer Wirkung gegen die Beschäftigten die Datenerhebung, die Datenverarbeitung und die Datennutzung erlauben. Dies bedeutet, dass, im Rahmen des Bundesdatenschutzgesetzes, solche Regelungen sehr weitgehende Erlaubnisse für den Arbeitgeber zur Kontrolle und Überwachung der Arbeitnehmer schaffen können. Dies gilt insbesondere für Fragen der Verhaltens- und Leistungskontrolle im Betrieb, so z. B. die Frage der Videoüberwachung von KassiererInnen, der Videoüberwachung von Beschäftigten insgesamt, dem Mitlesen von E-Mails, dem Aufzeichnen von Internetrecherchen durch Beschäftigte, dem Mithören und Mitaufzeichnen von dienstlichen Telefongesprächen und deren Auswertung zur Festlegung von Entlohnung und Beurteilung.

Betriebsräte sind aber in ihrer Arbeit schlicht erpressbar. Eine häufige Erfahrung ist, dass Betriebsräte mit dem Verlust von Arbeitsplätzen, dem Outsourcing von Betriebsteilen bedroht werden und ihnen gleichzeitig angeboten wird, dass von solchen Maßnahmen abgesehen werden kann, wenn sie bereit sind sehr weitgehende Regelungen hinsichtlich der Überwachung von Beschäftigten zuzustimmen.

Problematisch gestaltet sich auch die Erhebung von Daten, soweit der Arbeitnehmer dieser Erhebung im Arbeitsvertrag oder in sonstigen Vereinbarungen zwischen ihm und seinem Arbeitgeber zugestimmt hat. Nach der einschlägigen EG-Richtlinie können solche Zustimmungen nur dann wirksam erteilt werden, wenn diese „ohne Zwang“ abgegeben werden. Vor diesem Hintergrund hat der deutsche Gesetzgeber in das Bundesdatenschutz eine Regelung aufgenommen, die darauf abstellt, dass die Einwilligung „auf der freien Entscheidung des Betroffenen“ beruhen muss und erfüllt damit die Vorgaben der EG-Richtlinie. Nun wissen wir alle, dass insbesondere im Zeitpunkt des Abschlusses eines Arbeitsvertrages, von einer freien Willensentscheidung des betroffenen Arbeitnehmers keine Rede sein kann. Niemand wird den Abschluss eines Arbeitsvertrages gefährden, in dem er eine solche „freiwillige“ Zustimmung nicht erteilt. In der Bundesrepublik wird deswegen ganz überwiegend die Position vertreten, dass einer Einwilligung durch ein Arbeitnehmer in der Regel die „Freiwilligkeit“ fehlt und deshalb ein Arbeitnehmer auch nicht wirksam in die Datenerhebung einwilligen kann.

Bestehen jedoch Regelungen zwischen dem Betriebsrat und dem Arbeitgeber, sind diese an das verfassungsrechtliche Gebot des Persönlichkeitsschutzes gebunden. In der Regel fehlt es hier

jedoch am Kläger, der die Unwirksamkeit solcher Vereinbarungen, die das Persönlichkeitsrecht verletzen, geltend macht, da – wie oben gezeigt – die Betriebsräte zum Abschluss solcher Vereinbarungen erpresst worden sind und aus Angst vor der Gefährdung von Arbeitsplätzen selten ihre Rechte wahrnehmen. Geschieht dies im Ausnahmefall einmal, so wie es ein Betriebsrat der Deutschen Post im Jahr 2003 getan, der sich gegen eine im Rahmen einer Zwangsschlichtung zustande gekommenen Betriebsvereinbarung mit dem Argument gewandt hat, dass hier das Persönlichkeitsrecht der Beschäftigten verletzt wird, so können sie durchaus vor dem höchsten deutschen Arbeitsgericht Erfolg haben. Dieses hat durchaus enge Voraussetzungen für die Zulässigkeit von Arbeitnehmerüberwachung gesetzt. Dieses ist jedoch angesichts der tatsächlichen Machtverhältnisse im Betrieb in den seltensten Fällen durchsetzbar.

Damit stellt sich die Situation in den Betrieben so dar, dass hier auf der Basis von entweder „freiwilligen“ Einwilligungen durch den Arbeitnehmer oder durch erpresste Betriebsvereinbarungen ein sehr weitgehender, zumindest formal, rechtmäßiger Eingriff in Arbeitnehmerrechte möglich ist und Persönlichkeitsverletzungen zugelassen werden.

Kommen wir zurück zu den oben geschilderten Datenschutzskandalen. Diese Skandale stellen eine Verletzung geltenden Rechts dar und waren auch nicht gerechtfertigt durch etwaige Betriebsvereinbarungen. Die Bedrohung, dass illegales Handeln aufgedeckt wird, ist gering. So ist es eher zufällig, dass solche Rechtsverstöße überhaupt auffällig werden. Eine systematische Überwachung der Arbeitgeber durch staatliche Behörden findet nicht statt. Zwar gibt es staatliche Beauftragte für den Datenschutz, diese sind jedoch in ihrer personellen Ausstattung sehr begrenzt und damit in ihren Möglichkeiten sehr eingeschränkt. Diese Aufsichtsbehörden sind darauf angewiesen, dass Missbräuche eher zufällig an die Öffentlichkeit gelangen und sie dann eingreifen können. Ermitteln die Behörden dann in solchen Fällen, können sie Strafen aussprechen. Regelmäßig stellt ein solches Vergehen eine Ordnungswidrigkeit dar, welches in bestimmten Fällen mit einer Geldbuße bis zu 300.000,00 EUR geahndet werden kann. In besonderen Einzelfällen kann auch über diesen Rahmen hinausgegangen werden, wenn der wirtschaftliche Vorteil aus der Verletzung der Persönlichkeitsrechte von Arbeitnehmern einen höheren wirtschaftlichen Vorteil gebracht hat. Diese Strafandrohung stellt bei Unternehmungen, die Millionengewinne machen, keine ausreichende Bedrohung dar. Das Bedrohungspotential, das von den Aufsichtsbehörden und den Strafvorschriften ausgeht, ist zu gering, als dass es tatsächlich abschreckend auf die Arbeitgeber wirken kann. Dies zeigt sich alleine darin, dass viele der o. g. Betriebe bereits mehrfach und in kurzen Abständen durch Verstöße gegen den Datenschutz von Arbeitnehmern aufgefallen sind. Hier zeigt, dass diese Unternehmen die Strafandrohung offensichtlich als so gering einschätzen, dass sie diese billigend in Kauf nehmen können. Dagegen hilft nur, solche Fälle in die Öffentlichkeit zu bringen und einen öffentlichen Skandal zu provozieren, der die Unternehmen – zumindest zeitweise – zur Zurückhaltung zwingt. Dabei kommt gerade Gewerkschaften eine wichtige Rolle zu.

Notwendig ist die Schaffung eines separaten Arbeitnehmerdatenschutzgesetzes, welches beim Schutz der Arbeitnehmer deutlich über die bisherigen Regelungen in der Bundesrepublik hinaus geht und die Schaffung eines Strafrahmens, der tatsächlich abschreckend wirkt.

Dieter Hummel

*Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,*

De voorbije weken en maanden kwamen in Duitsland een groot aantal schandalen aan het licht waarbij werkgevers het recht op privacy van hun werknemers geschonden hebben. Een kleine bloemlezing:

De Duitse spoorwegen (Deutsche Bahn) en Telekom hebben hun werknemers bespied en een aantal bankrekeningen laten natrekken; Daimler Benz heeft illegaal medische gegevens van werknemers verzameld, Lidl en Schlecker, twee grootwarenhuizen, hebben hun werknemers op illegale wijze geobserveerd met behulp van videocamera's, grote radio-zenders hebben bij de indiensttreding van werknemers bloedonderzoeken uitgevoerd.

Deze gevallen zijn in de openbaarheid geraakt, maar ze zijn slechts een klein deel van het misbruik van werknemers-gegevens in het alledaagse bedrijfsleven in Duitsland. Dagelijks worden –zonder dat dat breed openbaar wordt gemaakt- in warenhuizen de werknemers illegaal gecontroleerd met videocamera's, dagelijks worden e-mails die werknemers versturen meegelezen door de werkgevers zonder wettelijke toelating, er worden illegaal data verzameld m.b.t. ziektes en diagnoses van werknemers en dagelijks worden, eveneens zonder wettelijke toelating, bijvoorbeeld in call-centra telefoongesprekken van werknemers gecontroleerd.

Daarenboven wordt de privésfeer van werknemers ook dagelijks geschonden door wettelijk toegelaten maatregelen. Het is werkgevers op grond van „bedrijfsafspraken“ toegelaten een zeer vergaande observatie van werknemers door te voeren bijvoorbeeld met camera's of door in callcenters de gesprekken die werknemers met klanten voeren bijna volledig op band op te nemen en persoonsgericht te analyseren en eveneens de resultaten daarvan te gebruiken als basis voor evaluaties en verloning.

Men moet weten dat er in Duitsland geen specifieke wet bestaat die de gegevens van werknemers beschermt. De bescherming van werknemersgegevens wordt nu geregeld door de algemene wet ter bescherming van persoonsgegevens, (Bundesdatenschutzgesetz). Deze wet heeft in de loop van haar lange bestaan nauwelijks oog gehad voor privacybescherming van de werknemers. Pas tijdens de hierboven geschetste schandalen kwam met § 32 van het Bundesdatenschutzgesetz de bescherming van werknemersgegevens meer op de voorgrond, zonder dat dit voor een toereikende bescherming zorgde. Er wird enkel in het algemeen geregeld dat bespieding van werknemers enkel onder bepaalde voorwaarden toegelaten is. Die voorwaarden zijn echter zo algemeen en zeer ruim opgevat, dat zij geen daadwerkelijke bescherming van werknemers vormen.

Daarbij is van belang te begrijpen dat in § 4 van het Bundesdatenschutzgesetz, dat gaat over de toelaatbaarheid in het algemeen van data- verzameling, verwerking en gebruik, voorziet dat de verzameling en verwerking van data ondermeer toegelaten is, wanneer een rechtsregel dit voorziet. In die gevallen is dataverzameling ook zonder medewerking of buiten weten van de

betrokkene mogelijk. De overeenkomsten tussen de bedrijfsraden (Betriebsräte) en de werkgever, zogenaamde *bedrijfsovereenkomsten*, maken zo'n „rechtsregel“ uit. *Bedrijfsovereenkomsten* zijn in het Duitse recht regelingen tussen enerzijds de bedrijfsraad (de werknemersvertegenwoordiging die in het bedrijf verkozen is) en anderzijds de werkgever. Zij hebben een normatief karakter, en dus bevatten zij voor de werknemers regels die onmiddellijk van toepassing en dwingend zijn. Volgens § 4 lid 2 Nr. 1 van het Bundesdatenschutzgesetz kunnen zulke bedrijfsakkoorden met onmiddellijke werking de verzameling, verwerking en het gebruik van werknemersgegevens toelaten. Dat betekent dat in het kader van het Bundesdatenschutzgesetz, zulke regelingen zeer verregaande controle –en bespiedingsbevoegdheden kunnen verlenen aan de werkgever. Dat geldt in het bijzonder voor controle van gedrag en prestaties in het bedrijf, zo bijvoorbeeld de videobewaking van kassiersters en andere werknemers, het meelezen van e-mails, het registreren van het internetsurfen van werknemers, het meeluisteren met en opnemen van professionele telefoongesprekken en de beoordeling ervan met het oog op evaluatie en het vastleggen van verloning.

Bedrijfsraden zijn in hun werking ronduit chanteerbaar. Een veel voorkomende ervaring is, dat *bedrijfsraden* onder druk worden gezet met het verlies van arbeidsplaatsen, de outsourcing van delen van het bedrijf en dat men hen tegelijkertijd aanbiedt, van deze maatregelen af te zien als men bereid is in te stemmen met verregaande regelingen m.b.t. de controle op de werknemers.

Eveneens problematisch is dat een werknemer met gegevensverzameling kan instemmen in zijn arbeidsovereenkomst of andere overeenkomsten met de werkgever. Volgens de EG-richtlijn die deze materie regelt, kan zulke instemming enkel dan rechtsgeldig gegeven worden, als ze zonder dwang gebeurt. Tegen die achtergrond heeft de Duitse wetgever in de Bundesdatenschutz- wet een regeling opgenomen, die stelt dat de toestemming „op de vrije wil van betrokkene“ moet steunen en daarmee is dan de voorwaarde van de EG-richtlijn vervuld. Nu weten we allemaal dat juist op het ogenblik van het afsluiten van een arbeidsovereenkomst, er van vrije wil vanwege de betrokken werknemer geen sprake kan zijn. Niemand zal de totstandkoming van een arbeidsovereenkomst in het gedrang brengen door zulke „vrijwillige toestemming“ niet te geven. In Duitsland wordt dan ook overwegend het standpunt verdedigd, dat er in de regel een gebrek is aan „vrijwilligheid“ in de toestemming van de werknemer en dat bijgevolg de werknemer niet geldig kan instemmen met de dataverzameling.

Als er regelingen bestaan tussen de bedrijfsraad en de werkgever dan zijn deze gebonden aan het grondwettelijke recht op bescherming van de privésfeer.

Aangezien de *bedrijfsraden* bedreigd worden met verlies van arbeidsplaatsen en onder die druk privacyschendende akkoorden afsluiten, zijn er in de regel weinig klachten over ongeldigheid van deze akkoorden. Uitzonderlijk wordt er toch klacht ingediend en kunnen de klagers hun slag thuishalen voor het hoogste Duitse Arbeidsgerecht. Dit was het geval bij de *bedrijfsraad* van de Duitse Post in 2003. Die keerde zich tegen een bedrijfsakkoord dat tot stand gekomen was in het kader van een onderhandeling onder dwang en dat de privacy van de werknemers schendde. Het hoogste Duitse arbeidsgerecht stelt zeer strenge vereisten voor de controle van werknemers. Gelet op de daadwerkelijke machtsverhoudingen in bedrijven zijn die maar zelden effectief gegarandeerd.

Gevolg is dat in veel bedrijven op basis van ofwel „vrijwillige“ toestemming van de werknemer ofwel van via chantage bekomen bedrijfsakkoorden er een zeer verregaande, minstens formeel toegestane inbreuken op de rechten van werknemers en privacyschendingen toegelaten zijn.

We komen terug op de hierboven geschetste privacy-schandalen. In deze situaties was het geldende recht geschonden en wird die schending niet gerechtvaardigd door bedrijfsovereenkomsten.

Het risico dat dit soort illegaal handelen uitkomt is echter gering. Het is eerder bij toeval dat deze illegale praktijken aan het licht komen. Systematische controle van de werkgevers door een staatsinstelling bestaat niet. Weliswaar zijn er staatsambtenaren voor de privacybescherming, maar die beschikken maar over beperkt aantal personeelsleden, waardoor hun mogelijkheden beperkt zijn. Die controle-instanties zijn afhankelijk van het eerder toevallig aan het licht komen van misbruiken. Dan kunnen zij ingrijpen. Stelt de overheid in dat geval een onderzoek in, dan kan ze straffen uitspreken. Regelmatig wordt bij zulke overtreding een strafbaar feit vastgesteld dat in sommige gevallen met een geldboete tot 300.000,00 EUR bestraft wordt. In bijzondere gevallen kunnen deze boetes verder oplopen, wanneer het economische voordeel van de privacyschending van van werknemers een groter commercieel voordeel heeft opgeleverd.

Het risico om een boete te krijgen is voor ondernemingen die miljoenenwinsten maken geen voldoende bedreiging. De omvang van de bedreiging, die van toezichtsorganen en strafbepalingen uitgaat, is te gering om daadwerkelijk afschrikkend te werken op werkgevers. Alleen al het feit dat vele van de bovenvernoemde bedrijven al meermaals en in korte tijdspanne met inbreuken tegen de privacy van werknemers de aandacht getrokken hebben, toont dit aan. Die ondernemingen schatten blijkbaar de kans gestraft te worden zo laag in, dat ze die best kunnen nemen. Het enige wat daartegen helpt is zulke gevallen in de openbaarheid te brengen en er een publiek schandaal van maken dat de ondernemingen – minstens een tijdlang – dwingt tot terughoudendheid. Vakbonden spelen daarbij een belangrijke rol.

Er moet nodig een aparte wet ter bescherming van de persoonsgegevens van werknemers komen, die de privacy van de werknemer beter beschermt dan nu het geval is in Duitsland. Bovendien moet de wet tegelijk afdwingbaar zijn en met een strafstelsel dat daadwerkelijk afschrikkend werkt.

Dieter Hummel

Brief biography

“Dieter Hummel Rechtsanwalt in Berlin, Vorsitzender der Vereinigung demokratischer Juristinnen und Juristen, langjähriges Engagement im Datenschutz”

L'UTILISATION DE LA BIOMÉTRIE ET DES RFIDS DANS LE CADRE DE L'ESPACE EUROPÉEN DE LIBERTÉ, DE SÉCURITÉ ET DE JUSTICE: UNE AFFAIRE DE BALANCE OU UNE QUESTION DE DIGNITÉ?

Franck Dumortier

Résumé

Dans la présente contribution, l'auteur rappelle que les droits de l'Homme constituent la limite principale et le fondement de l'association politique et que ceux-ci découlent d'une caractéristique essentielle de l'être humain : sa dignité. Après avoir rappelé le sens de ce concept fondateur, l'auteur examine ses implications sur l'interprétation du droit au respect de la vie privée au regard de l'utilisation de RFIDs et de la biométrie au sein de l'espace JLS. Au vu de l'importance des risques de dérive, l'auteur argue que le droit au respect de la vie privée ne peut en aucun cas être mis en « balance » avec un prétendu droit à la sécurité. Afin de respecter la limite et la raison d'être du Pouvoir, les ingérences de l'autorité publique doivent respecter la dignité humaine et rester strictement nécessaires dans une société démocratique.

1 Introduction

Depuis la signature du Traité d'Amsterdam, un des objectifs fondamentaux de l'Union européenne est d'offrir à ses citoyens un espace de « *liberté, de sécurité et de justice* »¹ (ci-après « espace JLS ») sans frontières intérieures. L'« espace normatif » qui en découle couvre, d'une part, des matières relevant du régime communautaire (1er pilier)—à savoir les politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration, ainsi que la coopération judiciaire en matière civile—et, d'autre part, des matières relevant du régime intergouvernemental (3ème pilier) comme la coopération judiciaire et policière en matière pénale.²

Dans ce contexte, cinq ans après avoir adopté un premier programme de travail à Tampere afin d'atteindre ses objectifs, le Conseil en a lancé un second, en 2004 à La Haye, dont la mise en oeuvre s'étale jusqu'en 2010.

Ce dernier y rappelle que la question de la sécurité de l'Union européenne et de ses États membres se pose avec une acuité renouvelée, au vu notamment des attentats terroristes perpétrés aux États-Unis le 11 septembre 2001 et à Madrid le 11 mars 2004. Les citoyens d'Europe attendent à juste titre de l'Union européenne que, tout en garantissant le respect des libertés et des droits fondamentaux, elle adopte une approche commune plus efficace des problèmes transfrontières tels que l'immigration illégale, la traite des êtres humains, le terrorisme et la criminalité organisée, ainsi que de leur prévention.³

Afin de concrétiser ces ambitions « sécuritaires » inter-piliers allant de la lutte contre le terrorisme à la prévention et la répression de l'immigration illégale, le programme de La Haye prône avec insistance une approche innovante de l'échange transfrontière d'informations en matière répressive selon le principe de disponibilité,⁴ le renforcement du recours à Europol et Eurojust, l'utilisation des données des passagers

¹ Le traité de Lisbonne signé en 2007 et soumis actuellement à ratification dans les États membres le rappelle dans son article 2.2 selon lequel l'« L'Union offre à ses citoyens un espace de liberté, de sécurité et de justice sans frontières intérieures, au sein duquel est assurée la libre circulation des personnes, en liaison avec des mesures appropriées en matière de contrôle des frontières extérieures, d'asile, d'immigration ainsi que de prévention de la criminalité et de lutte contre ce phénomène ».

² Rappelons que depuis le Traité de Maastricht, l'Union européenne repose sur trois piliers : les Communautés européennes (1er pilier), la Politique étrangère et de sécurité commune (2ème pilier) et la coopération policière et judiciaire en matière pénale (3ème pilier). Ces piliers se distinguent avant tout par le mode de décision employé mais également par la compétence de contrôle de la C.J.C.E. Ainsi, dans le 1er pilier, la procédure de décision est de type « communautaire » et implique l'ensemble des institutions. Par contre, dans les deuxième et troisième piliers, elle est de type « intergouvernemental », et le rôle du Parlement est nettement plus effacé. La compétence de la C.J.C.E. est également plus limitée dans le cadre du 3ème pilier que dans le cadre du premier.

³ Programme de La Haye, p. 3, disponible à l'adresse http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_fr.pdf.

⁴ Conformément au programme de La Haye, ce principe signifie que « dans l'ensemble de l'Union, tout agent des services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions peut les obtenir d'un autre État membre, l'administration répressive de l'autre État membre qui détient ces informations les mettant à sa disposition aux fins indiquées [...] ». Il est par ailleurs souligné dans le programme que « les méthodes utilisées pour échanger les informations devraient exploiter pleinement les nouvelles technologies et être adaptées à chaque type d'information, s'il y a lieu, par le biais d'un accès réciproque aux banques de données nationales, de leur interopérabilité ou de l'accès direct (en ligne) ».

pour des impératifs de sécurité des frontières et de l'aviation et d'autres fins répressives, l'interopérabilité entre le Système d'information Schengen (SIS II), le Système d'information sur les visas (VIS) et EURODAC,⁵ ainsi que l'intégration « sans tarder, des identificateurs biométriques dans les documents de voyage, les visas, les permis de séjour, les passeports des citoyens de l'UE et les systèmes d'information ».⁶

Depuis lors, les vœux du Conseil sont loin d'être restés lettre morte. Outre la multiplication des bases de données européennes contenant des éléments biométriques,⁷ des efforts importants ont été menés en matière d'interopérabilité,⁸ d'interconnexion⁹—voire de centralisation—de celles-ci, la Commission européenne dévoilant, par exemple, que l'une de ses actions-clés pour 2008 consiste en l'établissement d'une « banque » d'empreintes digitales centralisée.¹⁰ Dans un même mouvement, on constate une importante inflation législative dans le domaine de l'échange d'informations,¹¹ appliquant notamment le principe de disponibilité au transfert automatisé des profils ADN et des empreintes digitales.¹² Par ailleurs, force est de constater l'intégration progressive de plus de moyens biométriques d'identification, non seulement dans les visas et les titres de séjour délivrés aux ressortissants de pays tiers¹³ mais également dans les passeports et documents de voyage délivrés par les États membres.¹⁴ Enfin, fait non-négligeable, ces documents d'identification sont de plus en plus souvent équipés de technologie RFID¹⁵ afin de faciliter leur lecture à distance.

⁵ EURODAC est un système de comparaison des empreintes digitales des demandeurs d'asile et des immigrants clandestins afin de faciliter l'application du Règlement Dublin II qui permet de déterminer l'État responsable de l'examen d'une demande d'asile. EURODAC est formé d'une unité centrale située à la Commission qui est équipée d'une base de données centrale complètement automatisée et informatisée, destinée à la comparaison des empreintes digitales, et d'un système de transmission électronique des données reliant chaque État participant à l'unité centrale. EURODAC a été mis en place par le Règlement no 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système EURODAC pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

⁶ Programme de La Haye, p. 4.

⁷ Les bases de données SIS II et VIS contiennent des photographies et des empreintes digitales et EURODAC contient des empreintes digitales. Une nouvelle proposition concerne la collecte d'empreintes digitales dans le cadre d'un système d'entrée/sortie applicable à tous les ressortissants de pays tiers (y compris ceux qui ne sont pas soumis à visa lors de leur première entrée sur le territoire). Voy. la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, 13 février 2008. Une autre proposition concerne la création d'un système européen automatisé d'identification criminelle par les empreintes digitales (AFIS) dans lequel seraient rassemblées toutes les données relatives aux empreintes digitales qui ne sont actuellement disponibles que dans les AFIS nationaux. Enfin, une dernière proposition concerne la mise en place d'un « Registre européen des documents de voyage et des cartes d'identité » dans lequel les États membres « introduiront aussi les données biométriques enrôlées lors de la demande ». Voy. la Communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, COM (2005) 597 final—non publiée au Journal officiel.

⁸ Voy. par exemple, la Communication de la Commission européenne, du 24 novembre 2005, sur le renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la justice et des affaires intérieures et sur la création de synergies entre ces bases, op cit. ; et la Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », op cit.

⁹ Voy. notamment la proposition visant à créer un système européen d'information sur les casiers judiciaires (ECRIS) en vue de compléter la future Décision-cadre relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres, COM (2008)0332.

¹⁰ Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions du 21 février 2007, Stratégie politique annuelle pour 2008, COM (2007) 65 final.

¹¹ Voy. par exemple, la Décision-cadre 2006/960/JAI du Conseil du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, la proposition de Décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité ; le Traité de Prüm, signé par sept États membres (Allemagne, Autriche, Belgique, Espagne, France, Luxembourg et Pays-Bas), Journal officiel C 71/35 du 28.03.2007 ; les Décisions 2008/615/JAI, 2008/616/JAI et 2008/617/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (intégrant le Traité de Prüm dans l'ordre juridique de l'UE). Voy. également la proposition de Décision-cadre du Conseil relative à l'organisation et au contenu des échanges d'informations extraites du casier judiciaire entre les États membres, COM (2005) 690 final.

¹² Voy. par exemple les articles 2 à 9 de la Décision 2008/615/JAI, op cit.

¹³ Règlement (CE) no 1030/2002 du Conseil, du 13 juin 2002, établissant un modèle uniforme de permis de séjour pour les ressortissants de pays tiers ; Proposition de Règlement du Conseil modifiant le Règlement (CE) no 1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, COM (2003) 0558—non publié au Journal officiel.

¹⁴ Règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres ; Décision de la Commission du 28 juin 2006 établissant les spécifications techniques afférentes aux normes pour les dispositifs de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, COM (2006) 2909 final, non publié au Journal officiel. Depuis août 2006, les États membres délivrent des passeports biométriques contenant l'image faciale numérisée du titulaire ; à partir du 28 juin 2009, les passeports contiendront également les empreintes digitales.

¹⁵ En vertu de la Décision de la Commission du 28 juin 2006, précitée, les États Membres sont tenus d'utiliser des puces RF (à radio fréquences) comme support de stockage dans leurs documents de voyage et leurs passeports.

Ces nouveaux moyens technologiques mis à disposition des politiques européennes relevant du volet « sécuritaire » de l'espace JLS traduisent la convergence de plusieurs phénomènes a priori hétérogènes les uns aux autres mais se renforçant mutuellement : le surgissement d'un nouveau « paradigme sécuritaire » mêlant les objectifs précédemment indépendants de la lutte contre le terrorisme et la criminalité et de la lutte contre l'immigration illégale,¹⁶ la collecte généralisée d'éléments biométriques dans un but d'identification¹⁷ et d'authentification¹⁸ « fiable » des individus, la transmission de ces éléments par radio fréquence (RFID)¹⁹ aux autorités jugées compétentes, l'interopérabilité des bases de données en vue de leur interconnexion et enfin un échange accru d'informations rendu possible grâce au principe de disponibilité. L'ensemble de ces caractéristiques préfigure un espace de justice, de liberté et de sécurité basé sur une large dissémination de « capteurs » (RFIDs et biométriques) permettant le contrôle à distance des individus grâce à des processus ubiquitaires, opaques et automatiques²⁰ de croisement de données présumées exactes.

Ce premier volet sécuritaire paraîtrait quelque peu Orwelien s'il n'était accompagné de mesures destinées à garantir les droits fondamentaux des personnes concernées, en particulier leur droit au respect de la vie privée. A ce sujet, l'article 61.1 du Traité de Lisbonne rappelle que « l'Union constitue un espace de liberté, de sécurité et de justice dans le respect des droits fondamentaux [. . .] ». Loin d'être une profession de foi purement formelle, cette exigence semble avoir largement été prise à cœur par les institutions. Outre les nombreuses dispositions relatives à la protection des données à caractère personnel dont regorgent les textes législatifs susmentionnés,²¹ la matière fait l'objet d'un maillage législatif fort complexe en droit européen. Les directives 95/46/CE²² et 2002/58/CE²³ s'appliquent aux domaines relevant du pilier communautaire, une proposition de décision-cadre²⁴ est en cours de négociation afin de couvrir les

¹⁶ A cet égard, le Conseil « Justice et affaires intérieures » qui s'est réuni à Luxembourg les 12 et 13 juin 2007 illustre bien cette confusion des objectifs entre criminalité, terrorisme et immigration. A cette occasion, le Conseil a en effet invité la Commission à présenter dans les plus brefs délais une modification du Règlement EURODAC afin de permettre aux services de police et aux services répressifs des États membres ainsi qu'à Europol d'avoir accès, dans certaines conditions, à EURODAC, base de données conçue initialement comme instrument pour l'application du Règlement de Dublin.

¹⁷ L'identification permet de connaître une identité d'une entité, c'est-à-dire de déterminer l'identité d'un individu au sein d'une certaine population, elle nécessite une « one-to-many comparison » afin d'identifier l'utilisateur parmi l'ensemble des personnes enregistrées. Voy. la définition proposée à l'ISO : « Recognizing an entity within some context with unique identity references and additional information that characterizes the entity » (<http://www.jtc1sc27.din.de/sce/SD6>).

¹⁸ L'authentification est un processus qui consiste à vérifier l'identité prétendue d'une personne donnée afin d'obtenir l'assurance que l'individu est bien la personne qu'il prétend être, elle ne nécessite qu'une « one-to-one comparison », une comparaison des données transmises avec l'information préalablement enrôlée appartenant à une seule personne. Voy. la définition de l'ISO : « Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication) » (ISO/IEC 18028-4 : 2005).

¹⁹ Dans son projet de Recommandation sur la mise en oeuvre des principes relatifs à la vie privée, la protection des données et la sécurité de l'information dans les applications soutenues par la RFID de février 2008, la Commission définit l'identification par radio fréquence (RFID) comme « l'utilisation d'ondes électromagnétiques ou d'un couplage de champ réactif dans la portion de fréquence radio du spectre pour communiquer en direction ou en provenance d'une étiquette à travers différents schémas de modulation et d'encodage, et cela en vue de lire de façon exclusive l'identité d'une étiquette radiofréquence ou d'autres données stockées sur elle ». La Commission a également rappelé son intérêt pour la technologie RFID dans sa Communication au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions sur « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique, COM (2007) 96 final.

²⁰ La Commission prévoit de mettre en place un système d'entrée-sortie dans l'UE au moyen de « barrières automatiques ». Les voyageurs de bonne foi et les ressortissants de l'UE qui possèdent un passeport électronique pourraient faire l'objet d'une vérification automatisée à leur arrivée via un dispositif qui effectuerait une comparaison entre les identifiants biométriques du voyageur d'une part, et les données biométriques intégrées dans les documents de voyage ou dans une base de données d'autre part. Voy. la Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », op. cit.

²¹ Voy. par exemple les articles 6, 7 et 17 de la proposition de Décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, précitée ; les articles 8 et 9 de la Décision-cadre 2006/960/JAI, précitée ; les articles 24 à 32 de la Décision-cadre 2006/960/JAI, précitée ; l'article 4 du Règlement (CE) no 1030/2002, précité et l'article 4 du Règlement (CE) no 2252/2004, précité.

²² Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31-50.

²³ Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JO L 201 du 31.7.2002, p. 37-47.

²⁴ Une proposition de Décision-cadre du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, COM (2005) 475 final, est d'ailleurs actuellement en cours de négociation.

matières relevant du 3ème pilier,²⁵ la convention d'application de l'accord de Schengen²⁶ contient des dispositions spécifiques sur la protection des données applicables au Système d'information Schengen, la convention Europol²⁷ contient entre autres les règles relatives à la transmission de données à caractère personnel par Europol à des États et des instances tiers et la décision créant Eurojust²⁸ prévoit les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel.²⁹

Tant le volet sécuritaire que celui relatif à la protection des données font donc l'objet d'une attention toute particulière de la part des institutions chargées de concrétiser l'espace de liberté, de sécurité et de justice. Depuis le traité d'Amsterdam, « droits fondamentaux » et « sécurité » sont ainsi devenus les deux termes principaux de l'équation qu'ont pour mission de solutionner les institutions européennes dans le respect des valeurs démocratiques chères à l'Europe.

Dans cet esprit, un groupe de travail (ci-après « Future Group »³⁰) a été mis sur pied par les ministres de l'intérieur et de l'immigration en vue de conseiller les institutions pour préparer le programme de travail post-La Haye. Afin de résoudre l'épineuse question des liens et rapports que doivent entretenir entre eux les concepts de « droits fondamentaux » et de « sécurité », le « Future Group » recourt à la métaphore de la « balance ». Dans son rapport, le groupe propose ainsi de « préserver le modèle européen dans le domaine des affaires intérieures en mettant en balance mobilité, sécurité et vie privée ».³¹

Certes, ce groupe n'est pas l'inventeur du concept de la « balance » dans le domaine qui nous intéresse, la notion faisant malheureusement partie du langage politique communautaire depuis quelques années.³² Nous restons cependant abasourdis de voir figurer, dans un document d'orientation officiel, la référence à la « balance »— un instrument de mesure du poids—comme outil permettant de résoudre la délicate équation impliquant « droits fondamentaux » et « sécurité ».

Dans la présente contribution, nous ne référons pas le travail des autorités de contrôle et n'examinerons pas, en tant que telle, la conformité de l'utilisation de RFIDs et de la biométrie dans l'espace JLS avec les

²⁵ Pour avoir un aperçu des difficultés relatives à la détermination des champs d'application respectifs de la Directive 95/46/CE et la proposition de Décision-cadre, voy. Dumortier/Poullet [15].

²⁶ Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République Fédérale d'Allemagne et de la République Française relatif à la suppression graduelle des contrôles aux frontières communes, JO C 239 du 22.09.2000, p. 19.

²⁷ Articles 104 à 118 de la Convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de Police (Convention Europol), JO C 316 du 27.11.1995, p. 2.

²⁸ Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JO L 63 du 06.03.2002, p. 1.

²⁹ Nous ne prétendons pas être exhaustif dans l'énonciation des normes appelées à régler d'une manière ou d'une autre l'ensemble des aspects particuliers de la protection des données à caractère personnel dans l'espace de liberté, de sécurité et de justice.

³⁰ Le « Future Group » est un groupe de travail informel mis en place en 2007, à Dresde, par les ministres de l'intérieur et de l'immigration en vue de préparer l'avenir de l'espace européen de justice, de liberté et de sécurité. La raison d'être du groupe fut de rédiger un rapport politique contenant des recommandations qui serviront de « source d'idées » à la Commission européenne et aux États membres dans la conception des politiques dans le domaine des affaires intérieures après 2010.

³¹ Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy, précité, p. 17. Selon le groupe, one priority for each proposal based on the post-Hague Programme (. . .) will be the reflection on how to balance mobility, security and privacy in a proportionate way. There is a need to overcome the stereotype of seeing security, mobility and privacy as opposing concepts which exclude each other. Therefore, under the post-Hague Programme, an intensive public debate including a substantial inter-institutional discussion involving the European and national parliaments will have to be launched on how to address the current equilibrium in a way that allows for significantly improved security, at the same time as equally enhanced privacy and mobility. Son rapport contient d'ailleurs non moins de 16 occurrences de cette notion.

³² En 2004, M. Frattini, Commissaire en charge de l'espace de JLS déclarait que « new balances must be found between privacy and security » (SPEECH/04/549 disponible à l'adresse <http://ec.europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/04/549&format=HTML&aged=1&language=EN&guiLanguage=en>). Le 7 septembre 2005, la présidence britannique de l'Union européenne rédigeait déjà un document de travail intitulé « Liberty and security, striking the right balance ». Utilisant à nouveau la métaphore de la balance, la Commission européenne lança un programme intitulé « Security and safeguarding Liberties » au sein des perspectives financières 2007–2013 (disponible à l'adresse http://ec.europa.eu/justice_home/funding/intro/funding_security_en.html).

normes européennes de protection des données à caractère personnel. Notons toutefois que tant le CEPD³³ que le Groupe de l'article 29³⁴ ont d'ores et déjà fait connaître leurs positions à propos de l'utilisation de ces technologies par les autorités publiques.³⁵

Notre propos consistera plutôt à rappeler, dans un premier temps, que les droits fondamentaux ont été conçus à l'origine comme autant de limites que de finalités de l'exercice du pouvoir par les autorités publiques (2.) et que l'ensemble de ces droits découlent d'une valeur incommensurable reconnue à l'être humain : sa dignité. Nous exposerons ensuite en quoi la généralisation de l'authentification et l'identification biométriques dans le cadre de l'espace JLS peut aller à l'encontre de cette valeur fondamentale (3.). Nous conjuguerons alors le droit à la protection de la vie privée et le droit à la protection des données à caractère personnel à la lumière de cette dignité fondatrice avant d'examiner en quoi l'utilisation des RFIDs et de la biométrie à des fins d'identification peuvent porter atteinte à ces droits (4.). Enfin, nous concluons que le concept de « balance vie privée-sécurité » relève d'un langage inapproprié par rapport à l'esprit des déclarations protectrices des droits de l'Homme. En effet, il ne peut y avoir immixtion des autorités publiques dans l'exercice du droit à la vie privée que pour autant que celle-ci constitue une ingérence digne et proportionnelle dans une société démocratique. Ce postulat mérite certainement d'être rappelé au regard de l'utilisation généralisée de RFIDs et de procédés d'identification et d'authentification biométriques par les pouvoirs publics dans un contexte d'interopérabilité et d'interconnexion croissant des bases de données (5.).

2 Le sens des droits de l'homme : la limite et la finalité de l'exercice du pouvoir

Lorsque l'on écrit sur des problématiques touchant aux droits de l'Homme, il n'est sans doute jamais inutile de rappeler leur sens normatif et le rôle qu'ils sont destinés à jouer dans une société démocratique.

³³ Le CEPD (Contrôleur européen de la protection des données) est une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et la vie privée et de promouvoir les bonnes pratiques dans les institutions et organes de l'UE.

³⁴ Le groupe dit « de l'article 29 » est un organe consultatif européen indépendant sur la protection des données et de la vie privée placé auprès de la Commission européenne, composé de représentants de chacune des autorités de protection des données de l'Union européenne. Le groupe a été établi en vertu de l'article 29 de la Directive 95/46/CE. Ses missions sont définies à l'article 30 de la Directive 95/46/CE.

³⁵ En ce qui concerne le Groupe de l'article 29, voy. notamment l'avis no 4/2007 sur le concept des données à caractère personnel, l'avis 6/2005 sur les propositions de Règlement du Parlement européen et du Conseil (COM (2005) 236 final) et de Décision du Conseil (COM (2005) 230 final) sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), et sur une proposition de Règlement du Parlement européen et du Conseil sur l'accès des services des États membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) (COM (2005) 237 final), l'avis 3/2005 sur la mise en œuvre du Règlement du Conseil (CE) No 2252/2004 du 31 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, l'avis 2/2005 sur la proposition de Règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM (2004) 835 final), le document de travail sur les questions de protection des données liées à la technologie RFID (WP 105), l'avis 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système Européen d'information sur les visas (VIS), le Document de travail sur la biométrie (WP 82). En ce qui concerne le CEPD, voy. notamment, l'Opinion du 16 septembre 2008 sur « the proposal for a Council Decision on the establishment of the European Criminal Record Information System (ECRIS) in application of Article 11 of Framework Decision 2008/XX/JHA », l'Avis du 26 mars 2008 concernant la proposition de Règlement modifiant le Règlement (CE) no 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, l'Avis du 20 décembre 2007 sur la Communication de la Commission au Parlement européen, au Conseil, au Comité Economique et Social et au Comité des régions intitulée « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique », l'Avis du 19 décembre 2007 sur l'initiative de la République fédérale d'Allemagne, en vue de l'adoption d'une décision du Conseil concernant la mise en œuvre de la décision 2007/.../JAI relative à l'approfondissement de la coopération transfrontière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontière, l'Avis du 20 janvier 2006 sur la proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, l'Avis du 19 octobre 2005 sur trois propositions concernant le système d'information Schengen de deuxième génération (SIS II).

Ecrivant à l'occasion du cinquantième anniversaire de la Déclaration universelle des droits de l'Homme (ci-après DUDH), Michael Ignatieff a pu affirmer que ces derniers apparaissent comme « le principal article de foi d'un monde qui ne croit presque à plus rien ». ³⁶ Suite à la seconde guerre mondiale, la méconnaissance et le mépris des droits de l'Homme qui « ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité », ³⁷ les 58 Etats Membres qui constituaient alors 'Assemblée générale des Nations Unies adoptent la DUDH, texte fondateur qui inspirera tant la Convention Européenne des droits de l'Homme (ci-après « CEDH ») que la Charte Européenne des Droits Fondamentaux. Dès l'origine, ils apparaissent comme des droits fondamentaux inhérents à l'existence même des êtres humains. ³⁸ De plus,—et c'est là d'une importance cruciale pour notre propos—, même si leur opposabilité peut être étendue à d'autres personnes, ³⁹ les droits de l'Homme sont à l'origine des droits dont le respect s'impose essentiellement à l'Etat. ⁴⁰ A cet égard, les droits de l'Homme ont d'abord été conçus comme un principe de limitation du pouvoir étatique. Ces droits ont en effet été interprétés comme autant de garanties de la liberté individuelle par rapport aux ingérences de l'Etat, lequel—on s'en était aperçu—avait tendance à devenir totalitaire lorsqu'il pouvait laisser libre cours à ses immixtions. Par conséquent, ainsi que l'atteste le troisième considérant de la DUDH, la violation des droits de l'Homme par les gouvernants est depuis considérée comme le plus sûr indice « de tyrannie et d'oppression ». ⁴¹ Enfin, les droits de l'Homme ont également été interprétés comme une finalité du pouvoir étatique ⁴² en ce que les autorités publiques se voient assignées la tâche d'assurer la jouissance effective de ces droits. ⁴³

C'est dans cette perspective que les droits de l'Homme ont été conçus et doivent encore être interprétés ⁴⁴ : ils sont la limite, la finalité principale, sinon le fondement même de l'association politique. En ce sens, les droits de l'Homme sont la consécration du principe selon lequel le Pouvoir et les politiques qui en découlent doivent être au service de l'Homme.

Or, ainsi que nous l'avons déjà fait remarquer, le programme de travail de l'espace JLS semble être de plus en plus axé sur la « balance » entre deux « intérêts » considérés comme également importants, à savoir le respect des droits fondamentaux, d'une part, et le désir de sécurité de l'autre. Il convient cependant de rappeler avec force, qu'au contraire du droit au respect de la vie privée,—protégé notamment par l'article

³⁶ Ignatieff [24], p. 6.

³⁷ Selon le second considérant de la DUDH, « la méconnaissance et le mépris des droits de l'homme ont conduit à des actes de barbarie qui révoltent la conscience de l'humanité et que l'avènement d'un monde où les êtres humains seront libres de parler et de croire, libérés de la terreur et de la misère, a été proclamé comme la plus haute aspiration de l'homme ».

³⁸ Gewirth [20], p. 1 ; Donnelly [14], p. 9, qui définit les droits de l'homme comme un ensemble de droits universels appartenant de manière égale à toutes les personnes, exclusivement en raison de leur nature d'êtres humains. Voy. également Haarscher [22], p. 168.

³⁹ Depuis Young, James and Webster c. Royaume Uni (du 13 août 1981), la Cour EDH reconnaît l'effet horizontal de la CEDH. (Voir §49 : « Although the proximate cause of the events giving rise to this case was [an agreement between an employer and trade unions], it was the domestic law in force at the relevant time that made lawful the treatment of which the applicants complained. The responsibility of the respondent State for any resultant breach of the Convention is thus engaged on this basis », cité par De Schutter, 2000) Voir aussi, notamment, X et Y c. Netherlands, 8978/80 (1985) Cour EDH (du 26 mars 1985), Series A, vol. 91 : « although the object of Article 8 (art. 8) is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference : in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life (see the Airey judgment of 9 October 1979, Series A no. 32, p. 17, para. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves ».

⁴⁰ Kervegan [26], p. 644, soulignant que « la thématique des droits de l'individu est le contrecoup de l'affirmation de l'Etat et de son empire sur les individus ».

⁴¹ Selon le 3ème considérant de la DUDH, « il est essentiel que les droits de l'homme soient protégés par un régime de droit pour que l'homme ne soit pas contraint, en suprême recours, à la révolte contre la tyrannie et l'oppression ».

⁴² Gerard [19], p. 28.

⁴³ Tugendhat [39], p. 362–363 suggérant que les droits de l'homme, en tant que droits moraux au sens fort, impliquent l'exigence de créer un Etat chargé d'assurer leur effectivité. Voy. également dans ce sens, Wildt [41], p. 134 et 142. T. Pogge soutient pour sa part que les droits de l'homme, en tant que droits moraux, requièrent la création d'un ordre institutionnel assurant leur satisfaction. Voy. Pogge [30], p. 51–54.

⁴⁴ Rappelons que la Convention Européenne des Droits de l'Homme de 1950 se considère elle-même comme une première mesure propre à assurer la « la garantie collective de certains des droits énoncés dans la Déclaration universelle » et que la Charte Européenne des Droits Fondamentaux réaffirme « les droits qui résultent de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales » . . . Par conséquent, la Charte des Droits Fondamentaux se situe dans la même perspective que celle de la Déclaration de 1948.

8 CEDH—, un droit fondamental à la sécurité ne fait l'objet d'aucune consécration juridique.

Bien sûr, outre le droit au respect de la vie privée, l'organisation politique a également le devoir d'assurer à chacun le droit « à la sûreté de sa personne ».⁴⁵ Cependant, il importe de signaler que ce droit à la sûreté signifie toute autre chose qu'un droit à la sécurité. Il implique, entre autres, un devoir pour l'organisation politique d'assurer à chaque être humain de ne pas être arrêté ni détenu arbitrairement. A cet égard, il est intéressant de relever que, paradoxalement, l'effectivité de ce dernier droit est rendue moins certaine suite à l'utilisation des technologies biométrique et RFID, particulièrement lors de périodes troubles. Notons, par exemple, que Marc Rotenberg a vivement critiqué la récente initiative militaire des Etats-Unis visant à utiliser des scanners mobiles afin de collecter les empreintes digitales et les iris de centaines de milliers d'Iraqiens dans le but de les profiler. Selon ce dernier, "the new system of biometric identification and secret profiles raises the very real possibility of future reprisals and killings on a far more widespread basis".⁴⁶ S'il est vrai que la situation politique actuelle en Irak diverge fortement du contexte européen, il n'en a toutefois pas toujours été ainsi. Rappelons, en effet, que sous l'occupation française durant la seconde guerre mondiale, tout comme en Irak actuellement, de nombreuses personnes avaient eu la vie sauve en utilisant de fausses identités. Or, comme nous le verrons plus bas, l'utilisation généralisée d'identifiants biométriques et de technologie RFID dans les documents de voyage couplée à des bases de données interconnectées rend bien plus difficile la dissimulation de l'identité et peut donc faciliter les contrôles discriminatoires ainsi que la détention arbitraire.

Quant à la « sécurité », celle-ci n'a jamais été conçue comme un « droit » ayant un « poids » équivalent à ceux consacrant, par exemple, la dignité et le respect de la vie privée. Deux raisons suffisent à justifier cette conception. Non seulement un « droit à la sécurité » serait susceptible de multiples interprétations contradictoires,⁴⁷ mais plus fondamentalement, dans la logique des déclarations fondamentales, c'est par le respect de l'ensemble des droits civils, politiques et socio-économiques qu'elles proclament que celles-ci visent à assurer à l'Homme la sécurité civile, politique et socio-économique qui lui revient. La sécurité et la paix par la liberté, tel est le credo des droits de l'Homme.⁴⁸

C'est cette logique que renverse Antonio Vitorino, ancien Commissaire européen en charge de la Justice et des Affaires intérieures, lorsqu'il déclare que « la sécurité ne se limite pas à la répression de la criminalité: c'est un moyen pour atteindre la liberté ».⁴⁹ Il est d'une importance cruciale pour la démocratie que la métaphore de la « balance » ne conduise pas à confondre la fin et les moyens : c'est par l'assurance étatique de la jouissance effective de ses droits que l'Homme peut espérer vivre en paix et en sécurité, et non le contraire.

En adhérant aux instruments de protection des droits de l'Homme, c'est à cet engagement qu'ont souscrit les institutions européennes. Tant dans la conception que dans la mise en oeuvre de leurs politiques, elles ont pour obligation de respecter les droits de l'Homme en tant que limite et fondement du pouvoir afin que la finalité de celui-ci reste au service de l'Homme et de ses droits. C'est pourquoi elles doivent s'atteler à atteindre leur objectif de sécurité par le respect effectif des droits à la dignité et au respect de la vie privée,

⁴⁵ Voy. art. 3 de la DUDH.

⁴⁶ Voy EPIC, http://epic.org/privacy/biometrics/epic_iraq_ditbs.pdf.

⁴⁷ Parle-t-on de sécurité sociale, politique, économique, culturelle, psychique, juridique ou physique?

⁴⁸ Voy. notamment le préambule de la CEDH selon lequel « les libertés fondamentales constituent les assises mêmes de la justice et de la paix dans le monde ».

⁴⁹ Voy. http://ec.europa.eu/archives/commission_1999_2004/vitorino/index_en.htm.

au risque de confirmer la thèse bien connue d'Agamben et de Carl Schmitt selon laquelle l'« état d'exception » est la véritable source du droit.⁵⁰

3 La dignité humaine : l'Homme en tant que fin en soi

Si les droits de l'Homme sont reconnus en 1948 à tous « les membres de la famille humaine », ⁵¹ c'est parce qu'ils sont un ensemble de valeurs et d'intérêts dont le respect est jugé indispensable pour garantir la dignité humaine. L'homme ayant cruellement démontré sa capacité aux pires excès, il était important de rappeler solennellement et avec force le respect que mérite tout être humain du seul fait qu'il est être humain.⁵² C'est cet objectif que poursuivent le préambule de la Charte de l'ONU qui réaffirme sa « foi dans les droits fondamentaux de l'homme, dans la dignité et la valeur de la personne humaine [. . .] » et l'article 1er de la DUDH selon lequel « tous les êtres humains naissent libres et égaux en dignité et en droits ». C'est également dans cette tradition que s'inscrit la Charte européenne des droits fondamentaux lorsqu'elle proclame en son article 1er que « la dignité humaine est inviolable. Elle doit être respectée et protégée ». De manière non équivoque, ces textes considèrent la dignité humaine comme le fondement des autres droits.⁵³

Bien que la notion de dignité ne fasse l'objet d'aucune définition légale, elle connaît néanmoins une histoire longue de près de neuf siècles qui permet de la cerner quelque peu. La formulation d'un attribut humain fondamental en termes de dignitas trouve en effet sa source dans la pensée de la Renaissance.⁵⁴ Elle réapparaît au Moyen-Age en 1487 lorsque Jean Pic de la Mirandole écrit son essai *De Hominis Dignitate* qui constitue sans doute la première grande affirmation de la dignité humaine. ⁵⁵ Au XVIIe siècle, c'est Pascal qui reprend le thème,⁵⁶ mais c'est surtout Kant, « l'homme de droit »⁵⁷ selon Jean Lacroix, qui prépare le mieux la notion juridique de dignité et dont la conception nous intéresse particulièrement pour notre propos, tant ce philosophe fut une source d'inspiration non négligeable pour les auteurs de la DUDH.⁵⁸

⁵⁰ Voy. Agamben [1] et Schmitt [38]. Selon Schmitt, « Est souverain celui qui décide de la situation exceptionnelle » et « il est impossible d'établir avec une clarté intégrale les moments où l'on se trouve devant un cas de nécessité (Notfall) ni de prédire, dans son contenu, ce à quoi il faut s'attendre dans ce cas ».

⁵¹ Le premier considérant de la DUDH stipule que « la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde ».

⁵² En incorporant dans le droit international positif des normes minimales de protection des droits de l'Homme, les rédacteurs de la Charte de l'ONU et de la Déclaration universelle des droits de l'Homme ont voulu éviter que ne se répètent les horreurs de la seconde guerre mondiale, symbole d'une violation massive et d'une ampleur sans précédent de la dignité humaine.

⁵³ Quant à la CEDH, si elle ne contient pas de références explicites à la « dignité humaine » en tant qu'objectif moteur, il semble néanmoins logique de présumer que sa philosophie est cohérente avec la défense de la « dignité humaine » selon les mêmes principes que les autres instruments internationaux relatifs aux droits de l'Homme. Cette déduction s'appuie sur l'adhésion aux valeurs et objectifs de la Déclaration universelle des droits de l'Homme affirmée dans le préambule de la CEDH et sur les décisions fréquentes de la Cour européenne des droits de l'Homme, dont la portée est générale et qui sont révélatrices des objectifs généraux de la Convention. Ainsi, dans l'affaire *Pretty contre Royaume-Uni*, la Cour a conclu que « la dignité et la liberté de l'homme sont l'essence même de la Convention ». De même, dans l'affaire *Gündüz contre Turquie*, la Cour a jugé que « la tolérance et le respect de l'égalité de dignité de tous les êtres humains constituent le fondement d'une société démocratique et pluraliste ».

⁵⁴ Le mot « dignité » en français est attesté vers 1155. Voy. Rey [34], p. 604. Il dérive du latin *dignitas*, lui-même traduction du grec *axia* que l'on traduit d'habitude par valeur ou axiôme, utilisé par Aristote pour « axiome », « principe premier de la raison », « ce qui est approuvé dès qu'énoncé ». De même racine, *axios*, que l'on peut traduire par « digne », signifie plus fondamentalement encore « ce qui a du poids par soi-même », « ce qui entraîne par son propre poids », ou encore « ce qui de la valeur par soi-même ». Voy. Fierens [17], p. 10.

⁵⁵ Pic de la Mirandole [29]. A cette époque, Pic de la Mirandole est aux prises avec les censeurs romains. Le texte représente un élément de sa défense. En résumé, pour Pic, la dignité de l'homme tient à sa liberté. Il n'y a pas d'abord une nature humaine, mais un mouvement, une sorte de pouvoir natal par lequel l'homme décide et réalise son essence. C'est dire que l'homme ne naît pas homme mais le devient, comme s'il était son propre créateur.

⁵⁶ Voy. Fierens [17], p. 11. « Pascal, en quête de la grandeur de l'Homme à travers sa misère même, affirmera un principe universel en ce sens qu'il vaut pour tous les hommes, et un principe particulier en ce sens qu'il différencie l'homme de toutes les autres créatures : « L'Homme est visiblement fait pour penser, c'est toute sa dignité et tout son mérite ». « Toute la dignité de l'homme est dans la pensée, mais qu'est ce que cette pensée ? Qu'elle est sotte ». « Ce n'est pas de l'espace que je dois chercher ma dignité, mais c'est du règlement de ma pensée ». « Toute notre dignité consiste donc en la pensée ».

⁵⁷ Lacroix [27], p. 66.

⁵⁸ Voy. par exemple l'article 1er de la DUDH qui rappelle que les êtres humains sont « doués de raison et de conscience », conditions essentielles, selon Kant, pour que l'Homme puisse être responsable de ses actes.

Selon Kant,⁵⁹

dans le règne des fins, tout a un prix ou une dignité. Ce qui a un prix peut être aussi bien remplacé par quelque chose d'autre à titre d'équivalent ; au contraire, ce qui est supérieur à tout prix, ce qui par suite n'admet pas d'équivalent, c'est ce qui a une dignité (. . .) mais ce qui constitue la condition qui seule peut faire que quelque chose est une fin en soi, cela n'a pas seulement une valeur relative, c'est à dire un prix, mais une valeur intrinsèque, c'est-à-dire une dignité.⁶⁰

Dans cette perspective, lorsque la DUDH reconnaît la dignité à l'Homme, elle s'oppose à ce que celui-ci se voit attribuer une valeur relative et par conséquent mesurable. Ainsi, la dignité humaine impose à l'État une limite fondamentale: celle de toujours considérer l'Homme comme une fin en soi ayant une valeur intrinsèque et absolue. Que penser, dès lors, de l'utilisation par les pouvoirs publics de la biométrie (du grec *bios* signifiant « vie » et *metron*, « mesure ») et de RFIDs à des fins de contrôle des frontières et de surveillance généralisée?

Rappelons que la biométrie⁶¹ consiste en la mesure des éléments physiques, comportementaux et génétiques des êtres humains en vue de les traduire en identifiants uniques, permanents (ils restent pratiquement inchangés au cours de la vie d'une personne) et universels (ils sont valables dans tous les contextes). Au sein de l'espace JLS, l'objet de la biométrie est donc de mesurer l'Homme de manière systématique afin de permettre sa comparaison à un « équivalent » (une empreinte digitale, une image faciale, un échantillon ADN) dans le but de poursuivre un intérêt sécuritaire par une identification réputée plus « fiable ».

De leur côté, les RFIDs permettent d'assigner diverses informations uniques à des objets—parfois sensibles comme les passeports—et de les lire à distance, de manière ubiquitaire et opaque, transformant petit à petit les voyageurs en des « antennes » émettant automatiquement des informations standardisées sans nécessairement le savoir. En tant que tels, les RFIDs ont ainsi tendance à remplacer l'Homme, à titre d'équivalent, comme vecteur principal d'informations.

Dans le cadre de l'espace JLS, la convergence de ces deux technologies peut dès lors avoir pour conséquence le remplacement des facultés participatives et narratives de l'Homme par l'interrogation systématique de « capteurs » transmettant automatiquement des informations perçues comme incontestables car liées à l'unicité d'une personne grâce à la mesure des parties inchangeables de son corps (*bios*). Dans cette perspective, l'utilisation combinée de ces technologies à des fins de contrôle aux frontières peut faire courir des risques sérieux à un bon nombre de droits fondamentaux reconnus « à tous les membres de la famille humaine »,⁶² citoyens européens ou non, en particulier ceux au respect de la vie privée, « de circuler librement et de choisir sa résidence à l'intérieur d'un État »⁶³ et « de quitter tout pays, y compris le sien, et de revenir dans son pays ».⁶⁴

⁵⁹ Kant revient au sens le plus originel de la dignité, le sens grec de « valeur en soi », sans équivalent ».

⁶⁰ Kant [25], p. 160–162. C'est Kant qui souligne.

⁶¹ Biométrie : technologie d'identification ou d'authentification qui consiste à transformer les caractéristiques biologiques, morphologiques et comportementales d'une personne comme les empreintes digitales, l'empreinte de la rétine, de l'iris, de la voix, la forme du visage et de la main en une empreinte numérique.

⁶² Voy. le Préambule de la DUDH.

⁶³ Art. 13.1 de la DUDH.

⁶⁴ Art. 13.2 de la DUDH.

Certes, la lutte contre la criminalité et l'immigration illégale peuvent être considérés comme étant des objectifs étatiques légitimes, mais l'on peut néanmoins s'interroger sur la dignité du moyen utilisé qui pourrait aboutir au remplacement généralisé des facultés participatives et narratives de l'Homme par des processus d'échanges automatiques d'informations liées à la mesure des caractéristiques uniques de ceux-ci. La dignité de l'Homme ne peut être le prix, la mesure du désir de sécurité, puisqu'elle en est dépourvue.

La question est d'autant plus concrète étant donnée la généralisation de l'utilisation des technologies biométriques et RFID dans les passeports et les bases de données liées à l'immigration. En ce qui concerne ces dernières, rappelons que le système d'information sur les visas (VIS) peut contenir des données relatives à 70 millions de personnes, parmi lesquelles des empreintes digitales. De son côté, le système d'information Schengen (SIS) contenait 22 millions d'entrées au 1^{er} janvier 2008, dont des empreintes digitales. Enfin, dans la seule année 2006, EURODAC a traité 165 958 séries d'empreintes digitales de demandeurs d'asile, 41 312 séries d'empreintes digitales de personnes ayant franchi les frontières irrégulièrement et 63 341 séries d'empreintes digitales de personnes arrêtées alors qu'elles se trouvaient en séjour irrégulier sur le territoire d'un État membre.⁶⁵

Au vu de la généralisation des techniques biométriques et RFID, l'on peut légitimement se demander si ce sont encore les politiques européennes de lutte contre la criminalité et contre l'immigration illégale qui sont au service de l'Homme ou si, au contraire, ce n'est pas l'Homme qui devient le moyen de réalisation de celles-ci. Si l'on peut admettre que l'identification biométrique d'un être humain n'a pas pour vocation de le ramener à ses identifiants, son objectif premier est toutefois de déterminer ou de vérifier l'identité réelle ou prétendue d'un individu par ses identifiants corporels afin de lui appliquer les politiques appropriées et « de prendre les mesures adéquates ». ⁶⁶ L'Homme devient ainsi le moyen de la fin politique sécuritaire lors même que, dans la philosophie des droits de l'Homme, c'est sur lui que cette fin politique devrait être axée.

En effet, selon Kant, si l'humanité est par elle-même une dignité c'est parce que « l'Homme ne peut être traité par l'homme, comme un simple moyen, mais il doit toujours être traité comme étant aussi une fin. C'est précisément en cela que consiste sa dignité (la personnalité) ». ⁶⁷

Pour Kant, la dignité de l'Homme en tant que fin en soi implique donc également le respect de sa « personnalité ». Or, dans un contexte d'interconnexion et d'échanges accrus d'informations permettant de confronter les caractéristiques physiques d'un individu à des bases de données de manière instantanée par des procédés informatiques, la biométrie contient en germe le risque d'un glissement de l'identification à la réalisation de « background checks » contrôlant les comportements, les conduites et donc la personnalité des Hommes par le biais de données corporelles objectivées. Dans ce contexte, l'adjonction de capteurs RFID permettant une lecture ubiquitaire et quasi-automatique—parfois invisible et souvent opaque—d'informations d'identité prétendument infaillibles réduit encore la participation active et narrative de l'Homme au profit de ce qui est présumé être. Au sens sartrien, l'Homme est, il n'existe plus. Enfermé dans

⁶⁵ Commission européenne, communiqué de presse, « La base européenne de données biométriques continue de garantir une gestion efficace du régime d'asile européen commun », IP/07/1347, 18 septembre 2007.

⁶⁶ Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, op. cit., p. 9.

⁶⁷ Kant [25].

un canevas de données, l'Homme n'est plus considéré comme une fin en soi ayant activement une « personnalité », une « ipséité », ⁶⁸ c'est-à-dire une « identité » en tant que sujet réfléchi et narrateur participant à la construction de sa biographie. Au contraire, la biométrie peut avoir pour effet d'instrumentaliser le corps en le transformant en un moyen objectivable de connaissance de sa personnalité présumée dans le but de lui appliquer la politique sécuritaire appropriée. La personnalité active et narrative de l'Homme court dès lors le risque accru d'être emprisonnée dans un réseau de données identifiant sa « mêmété » dont il ne pourra s'échapper par narration, lors même que la dignité fondatrice de sa liberté réside dans son « ipséité ».

Les récentes propositions de la Commission pour une « stratégie de gestion intégrée des frontières » ⁶⁹ illustrent parfaitement les risques de dérives liés à la confiance aveugle en l'identification biométrique et dans les bases de données. Concrètement, la Commission prévoit l'instauration d'un « système d'enregistrement des entrées et sorties » ⁷⁰ des voyageurs et considère l'installation de barrières automatiques à la frontière qui rendrait possible une vérification automatisée de l'identité des voyageurs, sans intervention des gardes-frontières. Un appareil lirait les données biométriques figurant dans les documents de voyage ou stockées dans un système ou une base de données, et les comparerait aux identifiants biométriques du voyageur. Ce nouveau système « pourrait fonctionner sur la même plateforme technique que le SIS II et le VIS, en exploitant les synergies avec le système de correspondance biométrique (BMS), en cours de développement, qui pourrait constituer la base commune pour le système d'entrée/sortie, le VIS et le SIS II ». ⁷¹ De cette manière, ces barrières automatiques pourraient opérer automatiquement des contrôles ⁷² « dans le SIS et les bases de données nationales » ⁷³ afin de vérifier que les voyageurs ne sont pas de nature à compromettre l'ordre public, la sécurité intérieure, la santé publique ou les relations internationales de l'un des États membres.

Outre l'authentification des voyageurs en tant que telle, l'utilisation de la biométrie permettrait donc l'automatisation—au dépend des facultés narratives des êtres humains concernés—des procédures de consultation du SIS et de « bases de données nationales » dont on ignore la nature précise dans le contexte d'interopérabilité ambiant.

⁶⁸ La distinction entre « mêmété » et « ipséité » provient de P. Ricoeur. Selon ce dernier, le terme « identité » appliqué à un être humain peut désigner en français deux réalités différentes. La première concerne son corps dans son objectivité : à travers l'espace et le temps, à travers les lieux et les âges de sa vie, ce corps reste le même : c'est ce que l'auteur appelle la « mêmété ». C'est cet aspect que la biométrie permet de cerner : depuis la conception grâce à l'analyse génétique, jusqu'à la mort grâce aux données corporelles identifiantes obtenues de diverses manières—notamment grâce à des particularités morphologiques et à la photographie du visage. L'autre réalité concerne le vécu d'existence, par un sujet humain conscient et réfléchi. C'est le « soi-même », en anglais le « self ». On peut la désigner, pour la distinguer de la précédente, par le terme « ipséité », tiré du latin « ipse ». De ce point de vue, c'est le corps-sujet et non seulement le corps-objet qui est en cause, le corps tel qu'il se vit de l'intérieur et non pas tel qu'il se voit de l'extérieur. Cette réalité est certes subjective, mais c'est elle qui importe d'un point de vue éthique, car c'est elle qui rend possible l'exercice de la liberté. Voy. Comité Consultatif National (français) d'Éthique pour les Sciences de la Vie et de la Santé, Avis no 98, « Biométrie, données identifiantes et droits de l'homme », du 26 avril 2007, p. 7.

⁶⁹ Voy. Communication de la Commission au Conseil et au Parlement européen—« Vers une gestion intégrée des frontières extérieures des États membres de l'Union européenne », COM (2002) 233 final, 7 juin 2002, la Communication de la Commission du 13 février 2008 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée « Examen de la création d'un système européen de surveillance des frontières (EUROSUR) » COM (2008) 68 final—non publié au Journal officiel. Voy. également la Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, op. cit. Pour un commentaire de ces communications, Voy. Guild/Carrera/Geyer [21], disponible à l'adresse http://shop.ceps.eu/BookDetail.php?item_id=1622.

⁷⁰ Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, op. cit., p. 8.

⁷¹ Ibidem, p. 9.

⁷² En vertu du code frontières Schengen, la consultation du SIS est systématique pour les ressortissants de pays tiers mais ne peut être qu'aléatoire dans le cas des jouissant du droit communautaire à la libre circulation.

⁷³ Communication de la Commission, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », COM (2008) 69 final, op. cit., p. 4.

Or, lorsque l'on sait que Mr. et Mme. Moon⁷⁴ ont dû engager des procédures judiciaires durant 12 ans pour obtenir l'effacement des enregistrements illégitimes de leurs signalements du SIS, on comprend aisément en quoi l'aptitude narrative des êtres humains s'oppose à l'automatisation de la gestion des frontières quand des décisions aussi importantes qu'une interdiction de territoire, un renvoi ou une expulsion sont en jeu.⁷⁵

Bien sûr, il est généralement admis que pour pouvoir assurer ses missions d'intérêt général, l'Etat puisse reconnaître ses propres membres grâce à des données identifiantes extérieures, qui sont des données corporelles en quelque sorte rendues publiques, celles que nous appelons « état civil ». Elles permettent d'identifier dans l'espace public chaque citoyen par sa « mêmeité » et de le désigner : « c'est bien lui ».⁷⁶ Mais au vu de la multiplication et de la diversification des données d'identification biométriques, des techniques de collecte et de traitement de celles-ci, du paradigme sécuritaire de l'espace JLS basé sur une interopérabilité, une interconnexion—voire une centralisation—des bases de données et sur un échange accru d'informations grâce au principe de disponibilité, on peut s'interroger légitimement sur l'espace de liberté laissé à la personne, dans son « ipséité ». Là est la question éthique centrale dont nous examinons les implications juridiques dans les sections suivantes.

Ayant à présent rappelé que les droits de l'Homme constituent la limite et le fondement de l'action étatique et que cette limite et ce fondement imposent aux autorités de toujours respecter la dignité de l'Homme en tant que fin en soi, nous examinons dans la section suivante les conséquences qu'entraîne le respect de cette dignité fondatrice au niveau du droit à la protection de la vie privée et du droit à la protection des données à caractère personnel.

4 Le respect de la vie privée au regard de la dignité humaine : un engagement en faveur de l'autonomie par le biais de l'intégrité informationnelle

4.1 Le droit au développement social et relationnel de la personnalité

Si la dignité humaine a acquis une importance considérable au sein du cadre conceptuel qui régit les droits de l'Homme c'est parce que ceux-ci ont été conçus, dès l'origine, comme un bouclier de droits visant à empêcher toute entrave à la dignité humaine. Par conséquent, un droit de l'Homme particulier tel que celui qui protège le respect de la vie privée peut être qualifié de « droit au respect de la dignité »⁷⁷ dans la mesure où son objet est la défense indirecte de la dignité inhérente à l'Homme.

⁷⁴ Sur cette affaire, voy. Brouwer [9], disponible à l'adresse http://www.libertysecurity.org/IMG/pdf/The_Other_Side_of_Moon.pdf.

⁷⁵ A cet égard, les récentes propositions de la Commission poussent d'autant plus à la prudence lorsqu'elles prévoient que le système d'entrée/sortie vérifierait également le respect des délais de séjour des ressortissants de pays tiers et enregistrerait un signalement « accessible aux autorités nationales lorsque la durée de séjour autorisée dans l'UE est écoulée ». Un tel enregistrement automatisé de signalements peut, en effet, comporter un risque d'atteinte à la libre circulation de certaines catégories de personnes telles que les ressortissants de pays tiers introduisant par la suite une demande de regroupement familial, les ressortissants de pays tiers entrés sur base d'un visa touristique mais ayant obtenu par la suite le statut de résident de longue durée ou encore les demandeurs d'asile se trouvant légitimement sur le territoire de l'UE durant l'examen de leur demande d'asile. Pour toutes ces catégories de personnes, il est fort à parier que la lutte entre narration et traitement automatisé de signalements sur base de données biométriques ne sera pas gagnée d'avance.

⁷⁶ Comité Consultatif National (français) d'Éthique pour les Sciences de la Vie et de la Santé, op. cit.

⁷⁷ Feldman [16], notamment p. 689.

Un tel engagement en faveur de la dignité est intrinsèquement bidimensionnel, il y a d'une part son aspect absolu (le caractère moralement mauvais de la cruauté et de l'humiliation) et de l'autre un engagement en faveur de l'épanouissement humain (peut-être moins évident, mais tout aussi essentiel). Ces deux aspects sont liés, dans la mesure où chacun d'entre eux découle d'un engagement en faveur de la dignité humaine, qui se manifeste quant à lui dans des actes de compassion envers autrui. Sous sa forme prohibitive, le concept nous interdit la dépersonnalisation de nos semblables par des actes dégradants. Le côté positif qui met l'accent sur le développement et la réussite personnels, considère les droits de l'Homme comme étant radicalement pluralistes, dans le cadre de l'hospitalité envers les autres (et non la simple tolérance) qu'exige l'éthique qui le sous-tend. Considérés comme un tout, les droits de l'Homme sont par conséquent une idée qui, dans le même temps, nous protège en tant que personnes et nous permet de nous épanouir.⁷⁸

En tant qu'engagement envers l'Homme comme fin en soi, la dignité humaine comporte donc un aspect négatif, à savoir l'interdiction de la dépersonnalisation de l'Homme—la condamnation de la réduction de l'Homme à sa « mêmété »—et un aspect positif consistant en un devoir de promotion de l'épanouissement et de l'émancipation de l'Homme dans sa liberté, son « ipséité ».

Conçu comme un « droit au respect de la dignité », le droit à la vie privée est également lui-même tout naturellement bidimensionnel en soi. Ainsi, Agre a pu définir le droit au respect de la vie privée comme « la possibilité pour l'individu de construire sa propre personnalité à l'abri de contraintes excessives ».⁷⁹

Tant l'aspect négatif du droit à la protection de la vie privée,—l'absence de contraintes déraisonnables imposées par l'État ou des tiers—, que son aspect positif,—la possibilité de construire sa personnalité—, découlent de l'engagement fondamental en faveur de la dignité humaine. Loin d'être deux aspects poursuivant des objectifs normatifs distincts, ces deux versants soutiennent la même valeur finale, à savoir l'autonomie de l'Homme conçue comme « la capacité de l'Homme à maintenir et à développer sa personnalité d'une manière qui lui permette de participer pleinement à la société sans être poussé à conformer ses pensées, ses croyances, ses comportements et ses références aux pensées, croyances, comportements et préférences de la majorité ».⁸⁰ Cette valeur d'autonomie personnelle a été reconnue explicitement par la Cour EDH comme étant le principe interprétatif de l'article 8. Dans l'arrêt *Pretty*, la Cour considère ainsi que « bien qu'il n'ait été établi dans aucune affaire antérieure que l'article 8 de la Convention comporte un droit à l'autodétermination en tant que tel, [. . .] la notion d'autonomie reflète un principe important qui sous-tend l'interprétation des garanties de l'article 8 ».⁸¹

Cette autonomie personnelle ne doit cependant pas être perçue comme encourageant une « retraite et une indépendance radicales de la personne vis-à-vis de son environnement social mais bien plutôt comme l'autonomie d'une personne radicalement intégrée dans la société, vivant et communiquant avec d'autres personnes ».⁸² Ce droit à une vie privée relationnelle et sociale a été confirmée par la Cour EDH dans l'arrêt *Niemietz*, lorsqu'elle estime qu'il serait trop restrictif de limiter le droit au respect de la vie privée « à un « cercle intime » où chacun peut mener sa vie personnelle à sa guise et d'en écarter entièrement le

⁷⁸ Gearthly [18], p. 140–141.

⁷⁹ Agre/Rottenberg [2], p. 3.

⁸⁰ Rouvroy/Poullet [35], p. 15.

⁸¹ Cour EDH, *Pretty* c. Royaume-Uni du 29 avril 2002, §61.

⁸² *Ibidem*, p. 15.

monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables ».⁸³

Dans le même sens, la Cour EDH a jugé dans l'affaire *Pretty* que le droit au respect de la vie privée inclut « le droit au développement personnel et le droit d'entretenir des rapports avec d'autres êtres humains et le monde extérieur ».⁸⁴ Loin de constituer deux droits distincts, le droit au développement personnel et le droit d'entretenir des relations avec les autres sont intimement liés ainsi que le rappelle la Cour qui évoque le droit « d'assurer le développement de la personnalité de chaque individu dans ses relations avec ses semblables ».⁸⁵

Ce droit à l'épanouissement dans les relations sociales est également applicable aux ressortissants de pays tiers.⁸⁶ En effet, en se prononçant dans une affaire d'éloignement d'étrangers, le juridiction strasbourgeoise a considéré qu'en ayant « été éloignées du pays où elles avaient, sans interruption depuis la naissance, noué des relations personnelles, sociales et économiques qui sont constitutives de la vie privée de tout être humain », ⁸⁷ les requérantes avaient subi une ingérence dans leur « vie privée » au sens de l'article 8.

Dans la même perspective, dans l'arrêt *Boultif*, la Cour a estimé que « le refus de renouveler son autorisation de séjour en Suisse constitue une ingérence dans l'exercice par l'intéressé de son droit au respect de sa vie familiale, au sens de l'article 8 §1 de la Convention »⁸⁸ au motif qu'exclure une personne d'un pays où vivent ses parents proches peut constituer une ingérence dans le droit au respect de la vie familiale.

Ainsi, le respect effectif du droit à la vie privée exige de la part des autorités publiques non seulement le devoir de s'abstenir de restreindre la liberté considérée, mais également de prendre certaines mesures—telles que l'octroi d'un visa ou le renouvellement d'un permis de séjour. L'immigrant entré clandestinement sur le territoire d'un pays d'Europe comme le candidat réfugié débouté peuvent ainsi alléguer qu'un ordre d'expulsion—voire le refus de régulariser leur situation—constitue une ingérence dans leur vie privée

Enfin, la Cour a estimé qu'autonomie personnelle et développement personnel sont liés à l'identité, entendue comme le médium par excellence par lequel l'Homme noue des relations avec les autres. Comme telle, l'identité est ainsi protégée sur le terrain de l'article 8, la Cour déclarant que « le respect de la vie privée exige que chacun

puisse établir les détails de son identité d'être humain et que le droit d'un individu à de telles informations est essentiel du fait de leurs incidences sur la formation de la personnalité ».⁸⁹

C'est pourquoi, dans l'arrêt *Smirnova*,⁹⁰ alors que la Cour devait se prononcer sur l'incidence de la privation de passeport sur le respect du droit à la vie privée, elle estima

⁸³ Cour EDH, *Niemietz c. Allemagne* du 16 décembre 1992, §29.

⁸⁴ Cour EDH, *Pretty c. Royaume-Uni* du 29 avril 2002, §61.

⁸⁵ Cour EDH, *Botta c. Italie* du 24 février 1998, §32.

⁸⁶ Pour une étude plus générale de la jurisprudence de la Cour EDH relative à l'application de l'article 8 à des ressortissants de pays tiers, voy. Docquir [13], p. 921.

⁸⁷ Cour EDH, *Slivenko c. Lettonie* du 9 octobre 2003, §93.

⁸⁸ Cour EDH, *Boultif c. Suisse* du 2 août 2002, §40.

⁸⁹ Cour EDH, *Mikulic c. Croatie* du 7 février 2002, §54 ; voy. également *Gaskin c. Royaume-Uni*, arrêt du 7 juillet 1989, série A no 160, p. 16, §39.

⁹⁰ Cour EDH, *Smirnova c. Russie* du 24 juillet 2004.

que les citoyens russes doivent, dans leur vie quotidienne, faire état de leur identité particulièrement souvent, même pour accomplir des tâches aussi courantes que celles d'échanger de la monnaie ou d'acheter des billets de train. Le passeport interne est également nécessaire pour des besoins plus cruciaux, comme trouver un emploi ou recevoir des soins médicaux. Aussi la privation de son passeport a-t-elle représenté, pour Y.S., une ingérence continue dans sa vie privée.⁹¹

L'octroi conditionnel ou la privation d'un titre de séjour tout comme l'intégration de données relatives aux droits de séjour ou à l'identité d'un individu dans des bases de données publiques⁹² (EURODAC, VIS, etc.) constituent donc, en eux mêmes, des ingérences dans la vie privée des personnes concernées, qui, pour être justifiables aux yeux de la Convention, doivent être conformes au triple critère de l'article 8, §2.

Dans le contexte de l'utilisation de technologies biométriques et RFIDs dans l'espace JLS à des fins d'identification et de régulation de flux migratoires, cette réalité juridique mérite certainement d'être rappelée. Ainsi pour être conformes aux exigences de la CEDH, la généralisation d'identifiants biométriques dans l'ensemble des bases de données liées à l'immigration et dans les titres de séjour ainsi que l'utilisation de RFIDs dans ces documents se doit de ne pas exacerber de manière disproportionnée l'ingérence que constituent, déjà en eux-mêmes, les documents et bases de données liées à l'identité et à l'immigration.

Or, ainsi que le rappelle le CEPD, les données biométriques sont particulières du fait de certaines de leurs caractéristiques vantées, à savoir « la possibilité d'une identification quasi-certaine (elles sont uniques pour chaque individu), leur permanence (elles restent pratiquement inchangées au cours de la vie d'une personne) et leur universalité (les mêmes « éléments » physiologiques se retrouvent chez tous les individus) ». ⁹³ Ces prétentions d'universalité, de pertinence et de permanence sont cependant largement surfaites et loin d'être absolues, rendant, par conséquent, les traitements basés sur des « preuves » biométriques hautement sensibles du fait de la confiance excessive qui peut leur être conférée.

D'une part, le caractère d'universalité des données biométriques doit être nuancé étant donné que la proportion de personnes dont les empreintes digitales ne sont pas exploitables pourrait s'élever jusqu'à 5% (en raison d'empreintes digitales illisibles ou faisant entièrement défaut).⁹⁴ Par conséquent, si l'on peut estimer à quelque 20 millions le nombre de demandeurs de visas en 2007, « près d'un million de personnes ne seront pas en mesure de suivre la procédure d'enregistrement « normale », ce qui aura des conséquences évidentes au niveau des demandes de visas et au niveau des contrôles aux frontières ». ⁹⁵

Enfin, l'identification biométrique étant, par définition, un processus statistique, il serait exagéré de considérer qu'elle assure une « identification exacte » des personnes.

L'authentification de personnes, par empreinte digitale, est ainsi affectée d'un taux d'erreur normal de 0,5 à 1%;

⁹¹ Ibidem, §97.

⁹² Dans l'arrêt Rotaru, la Cour rappelle que « tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter constituent une ingérence dans le droit au respect de sa vie privée garanti par l'article 8 §1 de la Convention ». Cour EDH, Rotaru c. Roumanie, 4 mai 2000, §46.

⁹³ CEPD, Avis du 23 mars 2005 sur la proposition de Règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (COM (2004) 835 final, p. 7).

⁹⁴ Sasse [37], p. 7, et United States General Accounting Office, Technology Assessment, « Using Biometrics for Border Security », GAO-03-174, novembre 2002.

⁹⁵ CEPD, Avis du 23 mars 2005, op. cit., p. 7.

par conséquent, le pourcentage des rejets injustifiés (False Rejection Rate) du système de contrôle aux frontières extérieures oscillera entre 0,5 et 1 %. Ce pourcentage varie en fonction d'un seuil déterminé par la politique des autorités compétentes en matière de gestion des risques (qui correspond à l'établissement d'un équilibre entre le nombre de personnes rejetées par erreur et acceptées par erreur).⁹⁶

Loin d'être purement formelles, les craintes liées une importance accrue ou exagérée accordée aux preuves biométriques ont d'ores et déjà été vérifiées dans certaines affaires, un avocat de Portland, par exemple, ayant été emprisonné en 2004 pendant deux semaines parce que le FBI avait établi que ses empreintes digitales correspondaient à des empreintes trouvées dans le cadre des attentats de Madrid sur un sac plastique ayant contenu le détonateur.

Pour ces raisons, le Groupe de l'article 29 a déjà exprimé des réserves concernant la constitution d'une base de données centrale dans laquelle seraient enregistrées les données biométriques de tout étranger demandeur d'un visa ou d'un titre de séjour à des fins de contrôles ultérieurs des immigrants illégaux, quand ces données seraient de telle nature qu'elles porteraient sur des éléments dont toute personne laisse des traces dans la vie quotidienne.⁹⁷

Cette prise de position du Groupe ne semble cependant pas avoir troublé la Commission outre mesure dans sa proposition, déjà évoquée, de mettre en place un système d'entrée/sortie aux frontières extérieures. Non seulement des « barrières automatiques » authentifieraient l'identité des individus par l'examen de leur document de voyage biométrique et effectueraient des contrôles dans des bases de données européennes et nationales, mais le système vérifierait également le respect des délais de séjour des ressortissants de pays tiers et enregistrerait un signallement « accessible aux autorités nationales lorsque la durée de séjour autorisée dans l'UE est écoulée ». ⁹⁸

Un tel traitement automatisé comporterait, selon nous, un risque sérieux d'atteinte au droit à la vie privée de l'ensemble des ressortissants de pays tiers qui pourraient se voir interdire l'accès à un territoire, et par voie de conséquence à un réseau de relations sociales, sur base d'informations erronées. De plus, le système pourrait avoir pour conséquence d'enregistrer illégitimement des signalements pour dépassement de délai de séjour chez certaines catégories de personnes, pourtant en situation régulière, telles que les ressortissants de pays tiers introduisant par la suite une demande de regroupement familial, les ressortissants de pays tiers entrés sur base d'un visa touristique mais ayant obtenu par la suite le statut de résident de longue durée ou encore les demandeurs d'asile se trouvant légitimement sur le territoire de l'UE durant l'examen de leur demande d'asile. Serait ainsi menacé le principe consacré au considérant 2 de la Directive 95/46, selon lequel

les systèmes de traitement de données sont au service de l'homme ; (. .) ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux

⁹⁶ Ibidem, p. 8.

⁹⁷ Groupe de l'article 29, Avis no 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS), p. 8.

⁹⁸ Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Préparer les prochaines évolutions de la gestion des frontières dans l'Union européenne », op. cit., p. 9.

de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus.

Non seulement le droit à la protection de la vie privée, lu à la lumière des principes de dignité et d'autonomie, implique-t-il le respect de l'épanouissement de chacun dans ses relations avec ses semblables et subséquemment une protection contre les ingérences disproportionnées des autorités dans la liberté d'aller et de venir des individus, mais il impose également, selon certains, un droit de pouvoir se comporter avec les autres de manière contextualisée.⁹⁹ Nous arguons, dans les sections suivantes, que c'est à l'égard de cette dimension contextuelle du droit à la protection de la vie privée que les RFID et la biométrie suscitent les plus importantes interrogations.

4.2 Le droit à intégrité contextuelle

Selon un arrêt précurseur de la Cour constitutionnelle allemande,¹⁰⁰ l'autodétermination de l'Homme présuppose que celui-ci

continue à disposer de sa liberté de décider d'agir ou de s'abstenir, et de la possibilité de suivre cette décision en pratique. Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée.

Cette nécessité d'autodétermination contextualisée permettant aux Hommes de décider de manière autonome et informée a également été mise en lumière par la Cour EDH, notamment dans l'arrêt *Guerra*,¹⁰¹ considérant que les familles concernées auraient du avoir accès à une information pertinente relative aux inconvénients en termes de pollution environnementale pour exercer librement leur droit à la vie privée dans leur choix d'élire domicile près d'un complexe industriel.

Dans l'esprit de la Cour, l'autodétermination de l'Homme suppose donc une liberté de poser des choix en contexte avec un minimum d'ingérence afin de s'épanouir dans ses relations avec les autres. Il en résulte que la manière dont l'Homme exerce sa liberté décisionnelle d'agir ou de s'abstenir ainsi que sa liberté d'épanouissement et de développement personnel dépendent du contexte géographique, temporel, social, culturel et intersubjectif dans lequel il évolue. Il y a près de quarante ans, Barker proposait déjà son concept de « behavior setting »¹⁰² pour désigner des modèles de conduite déterminés par une structure composée d'éléments physiques et sociaux qui interfèrent avec des données culturelles propres au contexte. La relation entre espace et comportement, à laquelle on préfère souvent le terme d'« action », est envisagée aujourd'hui comme une conduite adaptative qui se traduit par le choix d'une option s'inscrivant dans un système de contraintes et d'opportunités. Ainsi les « lieux » sont vus, non seulement comme des localisations dans l'espace mais aussi comme des catégorisations de l'expérience qui permettent à l'individu de se

⁹⁹ Nissenbaum [28].

¹⁰⁰ Cour constitutionnelle, 15 décembre 1983, EuGRZ, 1983, p. 171.

¹⁰¹ Cour EDH, *Guerra c. Italie*, 19 février 1998.

¹⁰² Barker [7].

représenter les actions qu'il est susceptible de mener dans cet espace et les moyens qu'il a d'y parvenir d'après la manière dont sont connues et appréhendées les opportunités et les contraintes contextuelles.¹⁰³

Dans cette perspective, le droit à la protection de la vie privée implique le droit pour l'« être multiple » de pouvoir faire évoluer son « soi » (et sa liberté décisionnelle d'agir et de s'abstenir) d'après des normes relationnelles plus ou moins formelles selon la situation contextuelle envisagée. Une telle protection de la contextualisation des comportements participerait, selon nous, à l'effectivité du « droit à pouvoir mener sa vie comme on l'entend avec un minimum d'ingérence »¹⁰⁴ tel qu'il a été consacré par le Conseil de l'Europe. En tant qu'instrument au service de l'autonomie, le droit au respect de la vie privée doit donc aussi être compris comme un « droit à l'intégrité contextuelle »¹⁰⁵ comprenant, le cas échéant, un droit à l'imprévisibilité inter-contextuelle.¹⁰⁶

A cet égard, l'utilisation de RFIDs par les pouvoirs publics pose un certain nombre de questions. Les principales inquiétudes quant au respect de l'« intégrité contextuelle » découlent de la nature même de la technologie RFID qui parle pour nous et qui consiste, en tant que telle, en une « technologie infrastructurelle » composée d'un certain nombre d'éléments reliées en réseau, à savoir l'étiquette, le lecteur, la base de données de référence et la base de données dans laquelle les données produites par l'association étiquette-lecteur sont conservées. Ainsi que le relève la Commission,

les RFID ne sont pas de simples étiquettes ou codes-barres électroniques. Lorsque les dispositifs sont reliés à des bases de données ou des réseaux de communication, comme l'Internet, cette technologie offre un moyen très puissant de fournir de nouveaux services et applications dans pratiquement n'importe quel environnement.¹⁰⁷

Pour cette raison, les RFID sont considérés par l'Union internationale des télécommunications (UIT) comme la passerelle vers une nouvelle phase de développement de la société de l'information, souvent appelée « Internet des objets », dans laquelle l'Internet ne met plus seulement en relation ordinateurs et terminaux de communication, mais quasiment tous les objets de notre environnement quotidien, qu'il s'agisse de vêtements, de biens de consommation, de cartes de transports ou même d'objets plus sensibles tels que les documents de voyage.

On parle d'ailleurs, notamment au sujet des RFIDs, d'« ubiquitous computing » ayant plusieurs caractéristiques. Il s'agirait tout d'abord d'

une technologie de l'ubiquité dans la mesure où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus anodins de notre vie quotidienne, nos déplacements, nos hésitations, notre

¹⁰³ Voy. notamment Canter [10] ; Prohansky/Fabian/Kaminoff [32] ; Altman/Low [3].

¹⁰⁴ Résolution 428 du Conseil de l'Europe « portant déclaration sur les moyens de communication de masse et les droits de l'homme » du 23 janvier 1970.

¹⁰⁵ Nissenbaum [28].

¹⁰⁶ Cette garantie d'intégrité contextuelle ne doit cependant pas être comprise dans une perspective individualiste mais comme un outil garantissant le fonctionnement démocratique et vivace de la société. En effet, la protection de l'imprévisibilité inter-contextuelle a pour but de sauvegarder toute une série de comportements, postures, attitudes, expressions et modes de vie qui, sans être illégaux ni dommageables à autrui, sont simplement inhabituels, originaux, bizarres, saugrenus ou tout bonnement « différents », et qui à l'aune d'une mondialisation accélérée se doivent d'être protégés au titre du pluralisme nécessaire à l'effectivité de la démocratie. En 1920, Zamiatine avait déjà perçu toute la richesse et la vivacité de ce qu'il appelle les « hérésies », selon celui-ci « le monde se développe uniquement en fonction des hérésies, en fonction de ceux qui rejettent le présent, apparemment inébranlable et infaillible. Seuls les hérétiques découvrent des horizons nouveaux dans la science, dans l'art, dans la vie sociale ; seuls les hérétiques, rejetant le présent au nom de l'avenir, sont l'éternel ferment de la vie et assurent l'infini mouvement en avant de la vie ». Zamiatine [42], p. 11.

¹⁰⁷ Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social et au Comité des régions sur « L'identification par radiofréquence (RFID) en Europe : vers un cadre politique, COM (2007) 96 final, p. 1.

consommation domestique. Cette technologie est ensuite une technologie largement invisible (« calm technology ») dans un double sens : elle fonctionne de manière opaque, invisible (nous ne connaissons pas le circuit d'information sous-tendant le fonctionnement de la puce : qui la lit? Quand? Quelles informations? Pour qui?), mais également elle apparaît comme le prolongement naturel même de notre action (la porte s'ouvre et l'ordinateur s'allume) mettant les choses à notre service. Enfin, cette technologie est dite « apprenante » (« learning technology »). Ses applications ont souvent en effet pour caractéristique d'adapter leur fonctionnement aux données obtenues de par leur utilisation.¹⁰⁸

Les caractéristiques d'opacité et d'ubiquité de la technologie RFID, liées à des risques évidents en matière de sécurité, font craindre, tout d'abord, un manque de transparence pouvant donner lieu à une collecte et à un traitement d'informations à l'insu des personnes concernées, mais aussi, plus fondamentalement, une atteinte à l'intégrité contextuelle de ces informations. En effet, l'aspect « communication sans fil » de l'étiquette, ainsi que la capacité de lecture hors de portée visuelle qui la caractérise, rendent floues les limites traditionnelles de « l'espace personnel », se traduisant généralement selon Hall¹⁰⁹ par la distance physique qui s'établit entre des personnes.

Un tel danger de dé-contextualisation des informations a été mis en lumière par des chercheurs du Réseau d'Excellence FIDIS¹¹⁰ dans leur déclaration de Budapest¹¹¹ présentant les résultats de leur étude sur les Documents de Voyage à Lecture Automatique (MRTD—Machine Readable Travel Documents). Selon ceux-ci,

à la différence des documents d'identité habituels, les DVLA européens peuvent être lus et interceptés jusqu'à une distance de 10 mètres du porteur, de façon transparente et sans contrôle interactif ; cette faiblesse est encore aggravée par un contrôle d'accès susceptible d'être contourné ou attaqué, de sorte qu'un tiers, autorisé ou non, peut y avoir accès pour identifier le porteur et le fichier afin de, par exemple, suivre à la trace les touristes dans un pays étranger.¹¹²

Après avoir mis en exergue les multiples voies de piratage (man in the middle, vol de clef, système basique de contrôle d'accès vulnérable à une attaque en force brute, clonage aisé des RFID contenus dans les documents de voyage, etc.), l'analyse des chercheurs de FIDIS conclut que « la combinaison de ces menaces et de ces faiblesses met sérieusement en cause la sécurité et la sphère privée des citoyens européens; ceci est tout particulièrement vrai si l'on considère le déploiement à grande échelle des DVLA actuels et leur longue durée de validité (jusqu'à 10 ans) ». ¹¹³ Ces mises en garde en matière de sécurité ont depuis lors été actualisées par plusieurs chercheurs¹¹⁴ démontrant, par exemple, que les passeports belges de première génération—c'est à dire ceux émis jusqu'en juillet 2006—ne sont munis d'aucun mécanisme de sécurité et ont pu être lus à distance en quelques secondes à l'insu de leur porteur. Quant aux passeports seconde génération, émis depuis juillet 2006 et équipés de mesures de sécurité—le Basic Access Control (BAC)—, les chercheurs ont également démontré qu'ils ont pu accéder au contenu de ceux-ci après

¹⁰⁸ Pouillet/Rouvroy [31], p. 5.

¹⁰⁹ Hall [23].

¹¹⁰ FIDIS (Future of Identity in the Information Society ou Futur de l'Identité dans la Société de l'Information) est un réseau d'excellence créé dans le cadre du sixième programme cadre de l'Union Européenne.

¹¹¹ La déclaration de Budapest de septembre 2006 est disponible à l'adresse http://www.fidis.net/fileadmin/fidis/press/budapest_declaration_on_MRTD.fr.pdf.

¹¹² Ibidem, p. 2.

¹¹³ Ibidem, p. 3.

¹¹⁴ Voy. notamment Avoine/Kalach/Quisquater [4].

seulement une heure.¹¹⁵ Pour continuer dans la même veine, Jeroen van Beek, chercheur en sécurité à l'Université d'Amsterdam, a également pu lire et cloner les puces RFID de deux passeports biométriques britanniques avant d'y remplacer les photos par celles d'Osama Ben Laden et de Hiba Darghmeh, morte en 2003 dans un attentat.¹¹⁶ Enfin, le Groupe de l'article 29 a lui-aussi identifié le risque de décontextualisation des informations liées à l'identité estimant que des

préoccupations s'appliquent lorsque des terroristes seraient en mesure de détecter des nationalités spécifiques dans des foules. L'intrusion dans la vie privée serait encore plus grave quand le dispositif lui-même contient des informations personnelles importantes comme par exemple des renseignements relatifs au passeport ou des informations hautement sensibles.¹¹⁷

Insérée dans des documents de voyage, la technologie RFID fait donc courir un risque sévère d'atteinte à l'intégrité contextuelle des informations d'identité des individus en ce qu'elle met ceux-ci dans l'incapacité de dire leur identité, de la circonstancier et de la contextualiser. En ce sens, elle est problématique : les individus ne savent plus ce qu'ils disent, à qui ils le disent, quand ils le disent et où ils le disent.

La dimension contextuelle du droit à la vie privée est non seulement mise en danger par l'utilisation de technologie RFID dans les documents de voyage mais également par la généralisation des éléments biométriques dans ces documents et dans des bases de données telles que le SISII, le VIS et EURODAC. En effet, étant donné que l'Homme fait évoluer son « soi » de manière circonstanciée selon la relation intersubjective envisagée mise en contexte, le reflet de la personnalité de l'Homme (les informations qu'il transmet et celles qui sont stockées et échangées à son propos) est également variable et multiple. L'Homme doit donc avoir la possibilité d'exercer son droit à l'auto-détermination pour décider quelles informations adéquates, pertinentes et non-excessives il divulgue eu égard à ses objectifs et à sa prévision de ce qui est légitimement su de lui dans ce contexte. A cet égard, l'utilisation de la biométrie dans le cadre de l'espace JLS pose un certain nombre de questions que nous analysons dans la section suivante.

4.3 Le droit à l'intégrité informationnelle individuelle

Alors que le droit à la protection de la vie privée est un droit reconnu à l'Homme, le droit à la protection des données à caractère personnel est conféré à une catégorie de destinataires sensiblement différente, à savoir les « personnes concernées ». ¹¹⁸ Le terme anglais de « data subjects » est éclairant à ce propos, tant il tend à mettre en exergue le fait que ce sont les sujets de données—les sujets de représentations—qui sont protégés par le droit à la protection des données à caractère personnel. Là où le droit à la protection de la vie privée participe à l'émancipation du «soi» humain multiple et potentiellement imprévisible, nous

¹¹⁵ Avoine/Kalach/Quisquater [5].

¹¹⁶ Voy. Timesonline, 6 août 2008, disponible à l'adresse <http://www.timesonline.co.uk/tol/news/uk/crime/article4467106.ece>.

¹¹⁷ Groupe de l'article 29, Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification), 19 janvier 2005, WP 105, p. 8.

¹¹⁸ Bien sûr, le droit à la protection des données à caractère personnel poursuit un objectif analogue au droit au respect de la vie privée, la Directive 95/46/CE stipulant expressément que celle-ci a pour objectif « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel ». Le droit à la protection des données à caractère personnel participe ainsi, entre autres, à la garantie de la survivance d'une certaine autonomie nécessaire dans une société démocratique.

arguons que la protection des données à caractère personnel tend à prémunir les «personnes virtuelles»¹¹⁹— ou plutôt les «dividus»¹²⁰ contextuels—de la dé-contextualisation de leurs représentations informationnelles.

Selon Danièle Bouvier, la personne virtuelle peut être vue, d’abord, comme une personne numérique.

Il s’agit d’un « groupe d’informations nominatives qui circulent dans un réseau, rendant ainsi l’individu concerné présent sous forme incorporelle ». La transformation de la personne physique en nombre, en numéro, c’est-à-dire sa « numérisation », crée une nouvelle logique d’identification qui se caractérise par une domiciliation abstraite où s’exprime une télépersonnalité.¹²¹

Reprenant la notion de personne virtuelle, les chercheurs du projet FIDIS ont pointé la multiplicité de celle-ci en estimant que « nowadays, we all have several (partial) identities in our daily life. These identities are based on roles, actions, activities and may vary also depending on the context. New technologies have a direct impact on the very concept of identity ».¹²²

Constatant cet éclatement de la personnalité physique en de multiples personnalités virtuelles, certains auteurs ont dès lors prophétisé la mort de l’individu. Afin d’exprimer ce passage de l’individu à celle du « dividu » en contexte informationnel, Deleuze écrit qu’« on ne se trouve plus devant le couple masse-individu. Les individus sont devenus des « dividiels », et les masses, des échantillons, des données, des marchés ou des «banques».¹²³ Depuis lors, dans leur best-seller mondial « Les Netocrates»,¹²⁴ Alexander Bard et Ian Soderqvist ont réutilisé le terme de «dividu». Selon ceux-ci,

un individu est un objet indivisible, tandis qu’un « dividu » peut être séparé en différents éléments, puis réassemblé pour former de nouvelles structures. Nous ne sommes plus des êtres « individuels », mais des dividus existant dans des contextes sociaux différents. Et, plus important, nous avons arrêté d’essayer d’être constamment « toujours le même », fidèle à notre « véritable moi ». Au contraire, nous nous délectons à apparaître différents selon les contextes. Nous avons abandonné l’idéal de la personnalité «monopsychique» pour lui préférer celui de la personnalité «schizoïde». Nous chercherons désormais des consultations en schizanalyse plutôt qu’en psychanalyse. C’est la mort sociologique du sujet cartésien ».¹²⁵

Dans le cadre d’une société de l’information comme la nôtre où l’accès à des lieux, à des services, à des droits sont basés sur des traitements de données contenues dans des banques de données contextuelles, l’« individualité » kantienne—au sens de pôle de subjectivité unique et cohérent—a donc tendance à faire place à des « dividualités » multiples—sans pour autant être toujours étanches entre elles—qui résultent des informations traitées dans un certain contexte social, relationnel et intersubjectif pour un certain objectif contextuel. Dans chaque contexte, chaque dividualité se voit attribuer un identifiant différent (tel numéro de client au supermarché, tel numéro de téléphone professionnel, tel numéro de téléphone privé, tel

¹¹⁹ Bourcier [8].

¹²⁰ Deleuze [12].

¹²¹ Bourcier [8], p. 865.

¹²² FIDIS, deliverable “D 2.13 Virtual Persons and Identities”, p. 24, disponible à l’adresse http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp2-del2.13_Virtual_Persons_v1.0.pdf.

¹²³ Deleuze [12].

¹²⁴ Bard/Soderqvist [6].

¹²⁵ Voy. l’entretien d’Alexander Bard dont les sont recueillis par Rémi Sussan, disponible sur le site www.laspirale.org.

pseudonyme sur un site de rencontres, tel numéro de dossier de demande d'asile, tel numéro de vignette visa, tel numéro de compte en banque, etc.), lui permettant de construire sa représentation contextuelle dans un mouvement réciproque avec les intervenants du contexte dans lequel elle s'inscrit pour obtenir l'accès à tel lieu, tel service ou tel droit. C'est dans ce passage de l'individualité à la dividualité que nous situons la nécessité d'un droit à la protection des données à caractère personnel assurant un rempart contre la dé-contextualisation informationnelle de représentations dividuelles construites en contexte. En tant que garantie de l'« auto-détermination informationnelle », ¹²⁶ la protection des données à caractère personnel participe à la liberté autonome de l'Homme « de faire des projets ou de décider » ¹²⁷ sans être soumis à aucune pression exagérée (ce qu'assure le droit à la protection de la vie privée) par la garantie qu'elle offre aux « dividos contextuels » (les « data subjects ») de pouvoir « prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées ». ¹²⁸

A la lumière de ce principe d'« intégrité informationnelle » peuvent être lues nombre de dispositions des instruments européens de protection des données. Il en va ainsi notamment de l'article 6 b) de la Directive 95/46 selon lequel les données doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités » exprimant l'idée que les représentations dividuelles ne peuvent être utilisées que dans le cadre d'un contexte déterminé, explicite et proportionné, et que celles-ci ne peuvent être réutilisées dans un contexte incompatible. Il en va de même pour l'article 5 c) d'après lequel les données traitées doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement » rappelant que les représentations dividuelles ne peuvent être basées que sur des informations strictement nécessaires aux objectifs contextuels. C'est encore le cas pour l'article 5 e) qui stipule que les données ne peuvent être « conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement », lequel article peut être interprété comme procurant aux représentations dividuelles une garantie d'intégrité informationnelle temporelle.

En somme, nous voyons le droit à la protection des données comme la garantie d'une certaine « intégrité informationnelle dividuelle » au service du droit au respect à la vie privée, conçu lui-même en tant qu'outil assurant l'« intégrité contextuelle » des Hommes en vue de favoriser les capacités d'autonomie de ceux-ci au nom de leur radicale dignité. C'est précisément cette dimension dividuelle du droit à la protection des données à caractère personnel que l'utilisation d'éléments biométriques dans les documents de voyages et les bases de données liées au contrôle des frontières extérieures remet en question. Nous distinguons deux principaux risques de dé-contextualisation : le premier découle des caractéristiques intrinsèques de l'identification et de l'authentification biométriques ; le second dérive du cadre institutionnel dans lequel cette technologie est utilisée.

¹²⁶ Sur cette notion, voy. Rouvroy/Poullet [36].

¹²⁷ Cour constitutionnelle, 15 décembre 1983, EuGRZ, 1983, p. 171.

¹²⁸ Ibidem.

En ce qui concerne le premier risque, il est évident qu'en utilisant les empreintes des parties interchangeables du corps réduites à des codes numériques uniques pour chaque « individu », permanents—car évoluant peu dans le temps—et universels car valables dans l'ensemble des contextes dans lesquels celui-ci évolue, la biométrie individualise l'ensemble des dividualités contextuelles et temporelles de l'Homme et risque potentiellement de dé-contextualiser celles-ci. En utilisant des « caractéristiques physiques uniques et particulières d'une personne pouvant—du moins théoriquement—lui être attribuées en tout lieu et en tout temps avec une certitude quasi absolue », ¹²⁹ la biométrie contient en germe un risque de « fonction creep » susceptible de pervertir une méthode d'identification en un système de surveillance dématérialisé portant sur tous les aspects du monde vécu.

Avec la biométrie, on entre dans l'ère de l'interopérabilité maximale et les frontières inter-contextuelles perdent de leur substance. Ce constat est d'autant plus frappant dans le cadre de l'utilisation de la biométrie pour le contrôle des frontières extérieures de l'espace JLS. Alors que traditionnellement, les activités de contrôle se déroulaient dans un espace physique bien délimité et facilement localisable comme la frontière ou la place publique, la biométrisation des contrôles virtualise ces lieux fixes. Or, il convient de remarquer

que contrairement au monde virtuel qui englobe totalement l'individu, le monde physique ne s'impose pas entièrement à lui. Caractérisé par une structure aléatoire et contingente, il le laisse libre d'entrer ou de ne pas entrer dans son territoire, à l'exemple de l'individu qui décide de ne pas voyager donc de ne pas traverser les frontières, lieux fixes de l'identification et de contrôle. Toutefois, avec la biométrisation des contrôles, une fois entré dans le monde virtuel de l'identification et de surveillance, l'individu n'aura plus la latitude de le quitter. Par l'inscription de ses empreintes biométriques dans les bases de données nationales et transnationales, il entrera dans un monde virtuel de contrôles dont par ailleurs il ne connaît pas vraiment l'existence. ¹³⁰

Un second risque de dé-contextualisation découle, non pas de l'utilisation en tant que telle des technologies RFID et biométriques, mais plutôt de la structure institutionnelle au sein de laquelle cette utilisation s'inscrit. Il va de soi que la technologie ne se réduit pas seulement à un dispositif technique, scientifique et symbolique, mais qu'elle est également conditionnée par le contexte dont elle est le produit. Or, le nouvel espace JLS est structuré autour d'un titre unique servant de base institutionnelle à deux contextes de déploiement de politiques sensiblement différents à savoir d'une part la gestion des flux migratoires et, d'autre part, la lutte contre la criminalité et la coopération judiciaire. ¹³¹

Un sérieux danger de dé-contextualisation des informations traitées au sein de l'espace peut dès lors découler de ce titre institutionnel unique qui peut avoir comme effet, si on n'y prend garde, d'assimiler le demandeur d'asile, le demandeur de visa ou encore l'immigrant illégal à un criminel ayant commis un délit suffisamment grave pour justifier une collaboration transfrontière entre autorités policières nationales.

¹²⁹ Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données élaboré par PRIVATIM, les commissaires suisses à la protection des données, octobre 2006, no 3.1.2.

¹³⁰ Ceyhan [11].

¹³¹ Comme en témoigne la structure du titre V du Traité sur le fonctionnement de l'UE, l'espace de sécurité, de liberté et de justice est structuré autour de trois grands pôles d'action. Un premier chapitre est consacré aux « politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration », un second à la « coopération judiciaire en matière civile » et un dernier à la « coopération policière et judiciaire en matière pénale ». Le nouveau Traité de Lisbonne réunit ainsi, sous un même titre, l'ancien titre IV (visas, asile, immigration et autres politiques liées à la libre circulation des personnes) du Traité CE et l'ancien titre VI (dispositions relatives à la coopération policière et judiciaire en matière pénale) du Traité UE.

Or, rappelons que dans nombre d'Etats Membres, le séjour en situation irrégulière n'est constitutif d'aucun délit. Tout récemment, le Commissaire aux droits de l'Homme¹³² constatait d'ailleurs

avec une inquiétude grandissante une tendance à soumettre au droit pénal, dans le cadre d'une politique de gestion des migrations, l'entrée et la présence clandestines de migrants. Une telle méthode de maîtrise des déplacements internationaux porte atteinte aux principes établis du droit international. Elle est aussi à l'origine de nombreuses tragédies humaines sans pour autant atteindre sa finalité qui est de maîtriser réellement l'immigration. [. . .] Cette idée est peut-être populaire chez les xénophobes, mais elle constituerait une mesure rétrograde.¹³³

L'assimilation des politiques migratoires et de lutte contre la criminalité ne s'arrête pas à leur institutionnalisation dans un titre unique. En effet, dès le programme de la Haye, le Conseil est d'avis que « si l'on veut assurer une protection optimale de l'espace de liberté, de sécurité et de justice, l'action—au niveau de l'UE comme au niveau national—doit être multidisciplinaire et concertée entre les autorités répressives compétentes, en particulier la police, les douanes et la police des frontières ». ¹³⁴

C'est dans ce contexte que le Conseil européen et le Conseil de l'Union européenne ont tous deux invité à plusieurs reprises la Commission à présenter des propositions visant à accroître l'efficacité et l'interopérabilité des bases de données européennes et à créer entre elles des synergies.

Poussant à l'extrême la confusion entre les domaines de la gestion de l'immigration et de la lutte contre la criminalité, la Commission a soumis, en 2006, une proposition pour permettre aux autorités des États membres compétentes en matière de sécurité intérieure et à l'Office européen de police (Europol) d'accéder au système d'information sur les visas (VIS) afin de leur permettre de mieux prévenir et détecter des infractions pénales, notamment celles liées au terrorisme.¹³⁵

Exerçant sa compétence d'avis, le CEPD n'a pas manqué de relever le phénomène de dé-contextualisation qu'implique l'accès des services répressifs au VIS en estimant que

l'octroi aux services répressifs de l'accès à des bases de données relevant du premier pilier, même s'il peut être justifié par la lutte contre le terrorisme, est loin d'être anodin. Il convient de ne pas perdre de vue que le VIS est un système d'information mis au point aux fins de l'application de la politique européenne en matière de visas et non comme instrument de répression. Un accès systématique constituerait en effet une grave violation du principe de limitation de la finalité. Il entraînerait une ingérence disproportionnée dans la vie privée des voyageurs qui ont accepté que leurs données fassent l'objet d'un traitement en vue d'obtenir un visa, et s'attendent à ce que ces données soient collectées, consultées et communiquées uniquement à cette fin.¹³⁶

¹³² Le Commissaire aux droits de l'Homme est une institution indépendante au sein du Conseil de l'Europe; sa mission est de promouvoir la prise de conscience et le respect des droits de l'homme dans les 47 Etats membres du Conseil de l'Europe.

¹³³ Commissaire aux droits de l'Homme, Point de vue : « Il est injuste de sanctionner pénalement les migrations », 29 septembre 2008, disponible à l'adresse http://www.coe.int/t/commissioner/Viewpoints/080929_fr.asp.

¹³⁴ Programme de La Haye, p. 4.

¹³⁵ Proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des États membres compétentes en matière de sécurité intérieure et par l'Office européen de police (Europol) aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière, COM (2005) 600 final, Non publié au Journal officiel.

¹³⁶ CEPD, Avis du 20 janvier 2006 sur la proposition de Décision du Conseil concernant l'accès en consultation au système d'information sur les visas (VIS) par les autorités des Etats membres compétentes en matière de sécurité intérieure et par Europol aux fins de la prévention et de la détection des infractions terroristes et des autres infractions pénales graves, ainsi qu'aux fins des enquêtes en la matière (COM (2005) 600 final), p. 2.

La tendance n'est pourtant pas prête d'être inversée puisque le Conseil « Justice et affaires intérieures » qui s'est réuni à Luxembourg les 12 et 13 juin 2007 a invité la Commission à présenter dans les plus brefs délais une modification du règlement EURODAC afin de permettre aux services de police et aux services répressifs des États membres ainsi qu'à Europol d'avoir accès, dans certaines conditions, à EURODAC, base de données conçue initialement comme instrument pour l'application du Règlement de Dublin.

5 Conclusion : *"in dubio, pro libertate"*

Tout au long des sections précédentes, nous avons essayé de décrire les diverses dimensions du droit à la vie privée et du droit à la protection des données à caractère personnel auxquelles l'utilisation de la biométrie et des RFIDs dans le cadre de l'espace JLS portent incontestablement atteinte. Nous avons tout d'abord rappelé que le droit au respect de la vie privée comporte le droit de pouvoir développer sa personnalité dans ses relations avec ses semblables et que, par conséquent, l'« identité » et les documents y afférant sont protégés sur le terrain de l'article 8. Ainsi, l'octroi conditionnel ou la privation d'un titre de séjour tout comme l'intégration de données relatives aux droits de séjour ou à l'identité d'une personne dans des bases de données publiques constituent en eux-mêmes des ingérences au droit au respect de la vie privée. Nous avons alors exposé en quoi les technologies biométrique et RFID exacerbaient ces ingérences par les effets de dé-contextualisation informationnelle que celles-ci impliquent. D'une part, l'inclusion de RFIDs dans les documents de voyage peut avoir pour effet de mettre les Hommes dans l'incapacité de dire leur identité, de la circonscire et de la contextualiser, et ce au mépris de leurs facultés narratives et participatives. Ensuite, l'inclusion d'éléments biométriques dans ces mêmes documents et dans les bases de données relatives aux contrôles aux frontières peut entraîner, on l'a rappelé, une confiance exagérée dans les preuves biométriques pouvant potentiellement entraîner des décisions aussi graves qu'une arrestation ou un renvoi sur base d'informations erronées. Enfin, l'interopérabilité maximale rendue possible grâce à la biométrie attise encore le phénomène de dé-contextualisation informationnelle dans un contexte institutionnel où « criminalité » et « immigration » sont diluées dans un concept unique de « sécurité », attribuant systématiquement des représentations informationnelles stigmatisantes aux ressortissants de pays tiers.

L'ingérence accrue dans le droit à la protection de la vie privée ainsi provoquée par l'utilisation des RFIDs et de la biométrie dans le cadre de l'espace JLS ne fait donc pas de doute. Cependant, faut-il le rappeler, le droit à la protection de la vie privée n'est pas un droit absolu. Dès notre introduction, nous évoquons d'ailleurs la propagation, au sein du monde politique européen, du concept de la « balance » comme outil permettant de résoudre l'équation entre les intérêts de « vie privée » et de « sécurité ». Nous avons toutefois rappelé que cette métaphore keynésienne était contraire à l'esprit des déclarations fondamentales qui fonde l'ensemble des droits de l'Homme sur l'incommensurable dignité de celui-ci. Il ne peut donc être question de « balance » entre un intérêt—aussi légitime soit-il—et un droit fondamental faute de « prix » pouvant lui être associé.

La métaphore de la « balance » peut, en outre, affecter de manière significative l'état de droit basé, nous l'avons rappelé, sur le respect des droits de l'Homme comme limite et fondement du Pouvoir. Ainsi que le

constate Peter Hustinx,¹³⁷

a message such as : “No right to privacy until life and security are guaranteed” is developing into a mantra suggesting that fundamental rights and freedoms are a luxury that security cannot afford.[. . .] the Home Secretary of the United Kingdom, Dr John Reid, called for human rights law to be rewritten, stating that “The right to security, to the protection of life and liberty, is and should be the basic right on which all others are based”. [. . .] This position could be potentially dangerous and may produce more problems than it seeks to solve. Not only does it reveal a lack of understanding of the current framework of human rights in general, and data protection legislation in particular, which both enable proportionate measures that are necessary for public security or defence, it also ignores the lessons learned about the abuse of fundamental rights from dealing with terrorism within Europe’s borders over the last 50 years. There should be no doubt that effective anti-terror measures can be framed within the boundaries of fundamental rights. It is these rights that need to be protected under all circumstances in a democratic society. In the past examples can be found in different parts of Europe where the failure to protect fundamental rights has served as source of continued unrest rather than ensure safety and stability.¹³⁸

Nous nous rallions à l’analyse du CEPD et souhaitons mettre en exergue que le « principe de précaution » apparu récemment au niveau européen en matière d’environnement ne peut en aucun cas légitimer l’introduction de technologies sécuritaires intrusives et le recours exponentiel aux bases de données, devenues le moyen d’anticipation des comportements « à risque ». Cet univers de « précaution » omniprésente est en effet incompatible avec l’esprit des déclarations fondamentales selon lequel, rappelons-le, les immixtions dans le droit au respect de la vie privée ne sont justifiées, au regard de l’article 8 CEDH, que lorsque celles-ci (A.) poursuivent l’un des buts légitimes visés à l’article 8, §2 et constituent (B.) des ingérences (C.) « nécessaires dans une société démocratique » pour la réalisation de la finalité légitime poursuivie.

A. Tout d’abord, l’article 8, §2 de la CEDH ne permet d’« ingérence » dans le droit fondamental au respect de la vie privée que lorsque celles-ci poursuivent l’une des finalités légitimes énoncées en son sein. Dans le cadre de l’espace JLS, l’utilisation de des technologies RFID et biométrique semble poursuivre deux grandes catégories de finalités différentes à savoir, d’une part, un but de coopération policière et judiciaire, et, d’autre part, une finalité de régulation des flux migratoires. En ce qui concerne la première catégorie, il ne fait pas de doute que la coopération en matière répressive et judiciaire puisse être rangée sous les vocables de « défense de l’ordre et prévention des infractions pénales », de « sûreté publique », voire de « sécurité nationale ». Quant à la finalité de régulation des flux migratoires, l’exercice de qualification est plus délicat. Si la protection du « bien-être économique du pays »¹³⁹ a parfois été invoquée comme but légitime justifiant la régulation des flux migratoires, des recherches sociologiques récentes indiquent toutefois que la main d’oeuvre clandestine joue un rôle non négligeable dans le fonctionnement des économies européennes

¹³⁷ Peter Hustinx est le contrôleur européen à la protection des données.

¹³⁸ CEPD, “Letters to the incoming presidency : fundamental rights are not captives of security”, 11 juin 2007, disponible à l’adresse

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2007/07-06-11_Letters_portuguese_presidency_EN.pdf.

¹³⁹ Cour EDH, arrêt *Berrehab c. Pays-Bas*, 21 juin 1988.

(secteurs de la construction, de la restauration, de l'agriculture).¹⁴⁰ Un débat sur cette question devant la Cour EDH serait le bienvenu.

- B. Ensuite, lorsque des intérêts tels que la « sûreté publique », la « sécurité nationale », la « défense de l'ordre et la prévention des infractions pénales » ou la protection du « bien-être économique du pays » entrent en concours avec le droit au respect de la vie privée, la poursuite de ceux-ci n'est autorisée, sous conditions, par la CEDH, qu'au titre d'une « ingérence ». Or, le terme « ingérence » provient à l'origine d'« ingerere » qui dès 1362 signifie en langue française « s'introduire indûment, sans en être requis ou en avoir le droit ».¹⁴¹ Ce côté très restrictif de la notion d'ingérence est d'autant mieux mis en valeur par sa traduction anglaise « interference » du latin « enterferer » (enter, entre et ferir, frapper, dérivé de forare : forer, percer) qui signifie aussi bien « entrechoquer » que « percer un trou dans ». Dans cette perspective, une « ingérence » réalisée au nom d'un des buts légitimes susmentionnés qui « s'entrechoque » avec le respect des droits de l'Homme, peut tout au plus avoir comme effet d'y « percer un trou ». Au vu de la généralisation de l'identification précise par biométrie et RFID, —dont nous avons démontré les risques—, de la propagation des bases de données contenant des éléments biométriques et de leur interconnexion, on peut dès lors se poser la question de savoir si la condition d'« ingérence » est encore respectée par les autorités européennes. L'ensemble du « maillage » sécuritaire mis en place dans le cadre de l'espace JLS n'a-t'il réellement pour effet que de « percer un trou » dans les droits à la dignité et au respect de la vie privée des personnes concernées? La dilatation croissante du « trou » dans le droit à la protection de la vie privée des Hommes, citoyens européens ou non, n'est-il pas un premier symptôme du passage, que nous évoquons plus haut, de la conception d'une « société en paix par le respect des libertés » à une « société libre par la sécurité »?
- C. Outre cette considération d'ordre étymologique, le principe de proportionnalité exige encore que l'« ingérence » des pouvoirs publics soit « nécessaire » dans une société démocratique. Par cette exigence, la CEDH impose aux autorités l'examen du caractère « nécessaire » de la mesure qu'elles prévoient de mettre en oeuvre en vue de parvenir à l'un des buts légitimes énumérés à l'article 8, §2. Dans sa jurisprudence, la Cour Européenne des Droits de l'Homme a estimé que le sens de l'adjectif « nécessaire » était intermédiaire entre, d'une part, « indispensable » et, d'autre part, « admissible », « normal », « utile », « raisonnable » ou « opportun »,¹⁴² étant entendu que le simple opportunisme n'est pas un motif suffisant. Pour être nécessaire, l'ingérence doit encore être justifiée par un « besoin social impérieux »¹⁴³ se rapportant à un ou plusieurs buts légitimes. L'action de l'Etat doit en outre se fonder sur « une appréciation acceptable des faits pertinents ».¹⁴⁴ L'examen du caractère « proportionné » de l'« ingérence » commande donc l'analyse d'une triple exigence de « nécessité », de « besoin social impérieux » et de « motifs pertinents et suffisants ».¹⁴⁵ En matière de surveillance, la Cour a ainsi déjà estimé que « le pouvoir de surveiller en secret les citoyens n'est tolérable [...] que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques ».¹⁴⁶ Il s'agit là du « degré minimal de protection voulu par la prééminence du droit dans une société

¹⁴⁰ Voy. Rea [33], p. 831, et références citées.

¹⁴¹ Trésor de la Langue Française Informatisé (TLFI), disponible à l'adresse <http://atilf.atilf.fr/tlf.htm>.

¹⁴² Cour EDH, arrêt Sunday Times du 26 avril 1979, série A no 3, §59.

¹⁴³ Ibidem.

¹⁴⁴ Cour EDH, arrêt Oberschlick du 23 juin 1991, série A no 204, §60.

¹⁴⁵ Cour EDH, arrêt Dudgeon c. Royaume-Uni du 22 octobre 1981, série A, no 45, §50 à 53.

¹⁴⁶ Cour EDH, arrêt Rotaru c. Roumanie, 4 mai 2000, §47.

démocratique ». ¹⁴⁷ Dans la même perspective, certains auteurs considèrent que « la règle de la proportionnalité postule l'exclusivité du moyen : non seulement la limitation de la liberté doit apparaître comme le seul moyen apte à atteindre le but autorisé, mais encore, parmi plusieurs mesures qui peuvent s'offrir à elle, l'autorité doit opter pour la mesure la moins restrictive ». ¹⁴⁸

Au vu de l'inflation législative, déjà mentionnée, dans les domaines qui nous intéressent et du nombre de propositions prescrivant l'utilisation d'éléments biométriques ainsi que l'introduction de la technologie RFID dans les documents de voyages— dont l'importance des risques combinés a été démontrée—, l'on peut légitimement se demander si le principe de proportionnalité—en tant qu'il impose la minimisation des données ainsi que la modération dans le choix de la technologie—a été respecté par les autorités responsables de l'espace JLS.

La complexité et le nombre d'initiatives dans les matières évoquées posent également certains soucis au CEPD qui avoue ne plus toujours être en mesure d'évaluer correctement la proportionnalité des propositions qui lui sont soumises, pour avis, par les autorités. Selon celui-ci,

regardless of the inherent merits of each proposal, the EDPS is concerned that far reaching proposals implying surveillance of the movements of individuals follow each other at an amazing pace. Many proposals have been or are about to be tabled in this area (SIS II, VIS, review of Eurodac Regulation, access of law enforcement agencies to these systems, PNR, etc.). All these proposed measures are intended to contribute to the monitoring of travellers before and upon entry to the EU (or Schengen) territory. The sheer number of these proposals and the seemingly piecemeal way in which they are put forward make it extremely difficult for the stakeholders (European and national Parliaments, data protection authorities including EDPS, civil society) to have a full overview. This limits the possibility to contribute meaningfully. There is for instance a risk that Data Protection Authorities might find a proposal acceptable only to discover later that it would actually be unacceptable when considered in synergy with the other, more recent proposals. The EDPS would like to see evidence that there is a master plan for all these initiatives, giving a clear sense of direction. Such a general plan would greatly help to analyse the impact of the totality of these measures on the travellers (in third countries, at entry or within the EU territory) and to design appropriate safeguards. ¹⁴⁹

Face à la complexité de l'analyse de proportionnalité résultant des synergies— parfois voulues, parfois non—entre, d'une part, les différentes propositions législatives, et, d'autre part, les différentes technologies utilisées, il n'y a, selon nous, qu'une réponse démocratiquement acceptable : « in dubio, pro libertate ». Les droits et libertés doivent faire l'objet d'une définition extensive, lors que les limitations susceptibles de leur être apportées doivent être interprétés restrictivement afin que la CEDH puisse continuer « de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs ». ¹⁵⁰

¹⁴⁷ Cour EDH, arrêt Kopp c. Suisse du 25 mars 1998, §75.

¹⁴⁸ Velu/Ergec [40], p. 120.

¹⁴⁹ CEPD, "Preliminary comments on three Communications from the Commission on border management (COM (2008) 69, COM (2008) 68 and COM (2008) 67)", 3 Mars 2008, p. 3, disponible à l'adresse http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2008/08-03-03_Comments_border_package_EN.pdf.

¹⁵⁰ Cour EDH, arrêt Airey v. Ireland du 9 octobre 1979, §22. Voy. également Cour EDH, arrêt Loizidou v. Turkey du 23 March 1995.

Bibliographie

1. Agamben, G.: *État d'exception. Homo sacer*, Seuil (2003)
2. Agre, P.E., Rottenberg, M. (eds.): *Technology and Privacy. The New Landscape*. MIT Press, Cambridge (1998)
3. Itman, I., Low, S.M. (eds.): *Place Attachment*. Plenum, New York (1992)
4. Avoine, G., Kalach, K., Quisquater, J.: *Visite guidée du passeport biométrique*. In: Dossier RFID, sécurité et vie privée, revue MISC, novembre 2007
5. Avoine, G., Kalach, K., Quisquater, J.: *Le passeport biométrique belge recalé au BAC. . . Vos informations personnelles sont en danger!*. Disponible à l'adresse http://www.dice.ucl.ac.be/crypto/passport/index_fr.html
6. Bard, A., Soderqvist, I.: *Netocracy: The New Power Elite and Life After Capitalism*. FT Press, London (2002)
7. Barker, R.: *Ecological Psychology*. Stanford University Press, Stanford (1968)
8. Bourcier, D.: *De l'intelligence artificielle à la personne virtuelle: émergence d'une entité juridique?*. *Droit Soc.* 49, 847–871 (2001)
9. Brouwer, E.: *The other side of Moon—the Schengen information system and human rights: a task for national courts*. CEPS Policy Brief No. 288, CEPS, avril 2008
10. Canter, D.: *The Psychology of Place*. Architectural Press, London (1977)
11. Ceyhan, A.: *Enjeux d'identification et de surveillance à l'heure de la biométrie*, *Cultures & Conflits*, 64, hiver 2006. Disponible à l'adresse <http://www.conflits.org/index2176.html>
12. Deleuze, G.: *Post-scriptum sur les sociétés de contrôle*. *L'autre J.* 1 (1990)
13. Docquir, P.-F.: *Droit à la vie privée et familiale des ressortissants étrangers : vers la mise au point d'une protection floue du droit de séjour ?*. *Revue Trimestrielle des Droits de l'Homme* 6/2004
14. Donnelly, J.: *The Concept of Human Rights*. Londres (1985)
15. Dumortier, F., Poulet, Y.: *La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne*. In: *Revue Lamy Droit de l'Immatériel*, issue 29, pp. 76–86
16. Feldman, D.: *Human dignity as a legal value—Part I (La dignité humaine en tant que valeur juridique, 1ère partie)*. *Public Law* (hiver), 682–702 (1999)
17. Fierens, J.: *Encombrante dignité humaine*. In: *Cahiers de la Faculté de droit de Namur*; 30 (2002)
18. Gearthy, C.: *Can Human Rights Survive? The Hamlyn Lectures 2005 (Les droits de l'homme peuvent-ils survivre ? Les conférences de Hamlyn 2005)*. Cambridge University Press, Cambridge (2006)
19. Gerard, Ph.: *L'esprit des droits—philosophie des droits de l'homme*. Publications des Facultés universitaires de Saint-Louis, Bruxelles (2007)
20. Gewirth, A.: *The epistemology of human rights*. In: Paul, E.F., Paul, J., Miller, F.D. Jr. (eds.) *Human Rights*. Oxford (1986)
21. Guild, E., Carrera, S., Geyer, F.: *The Commission's New Border Package: Does it take us one step closer to a 'cyber-fortress Europe'?*. CEPS Policy Brief No. 154, CEPS, Mars 2008
22. Haarscher, G.: *Droits de l'homme*. In: Raynaud, Ph., Rials, S. (dir.) *Dictionnaire de philosophie politique*. Paris (1998)

23. Hall, E.T.: *La dimension cachée*, 1ère éd. Doubleday, Garden City (1966)
24. Ignatieff, M.: *Droits de l'homme : la crise de la cinquantaine*. *Esprit* 255–256, 6–23 (1999)
25. Kant, I.: *Fondement de la métaphysique des mœurs* (1785)
26. Kervegan, J.-Fr.: *Les droits de l'homme*. In: Kambouchner, D. *Notions de philosophie II*. Paris (1995)
27. Lacroix, J.: *Kant et le Kantisme*. Coll. *Que sais-je?*, no 123. Presses universitaires de France, Paris (1969)
28. Nissenbaum, H.: *Privacy as contextual integrity*. *Washington Law Rev.* 79(1), 119–158 (2004)
29. Pic de la Mirandole, J.: *OEuvres philosophiques, texte latin, traduction et note par Olivier Boulnois et Giuseppe Tognon*. Coll. *Epiméthée*. Presses universitaires de France, Paris (1993)
30. Pogge, T.: *The international significance of human rights*. *J. Ethics* 4, 51–54 (2000)
31. Poulet, Y., Rouvroy, A.: *Ethique et droits de l'homme dans la société de l'information*, 13–14 septembre 2007. Strasbourg: *Rapport général introductif*, Council of Europe & UNESCO, Strasbourg (2007)
32. Prohansky, H., Fabian, A., Kaminoff, R.: *Place identity, physical world, socialization of the self*. *J. Environ. Psychol.* 3 (1983)
33. Rea, A.: *L'avenir de l'Europe : l'immigration sans fin*. *Rev. Droits Etrangers* 121 (2002)
34. Rey, A.: *Dictionnaire historique de la langue française*, éd. Le Robert (1992)
35. Rouvroy, A., Poulet, Y.: *The right to informational self-determination and the value of selfdevelopment. Reassessing the value of privacy for democracy*. In: *Reinventing Data Protection. Actes de la conférence internationale des 12–13 octobre 2007, à paraître*
36. Rouvroy, A., Poulet, Y.: *Self-determination as the “key” concept*. In: *Reinventing Data Protection, International Conference co-organized by the University of Tilburg, the Information Technology & Law Research Centre, University of Namur, and the Vrij Universiteit Brussels, 12–13 October 2007* (2007)
37. Sasse, A.: *Cybertrust and crime prevention: Usability and trust in information systems*. In: *Foresight Cybertrust and Crime Prevention Project*, 04/1151, 10 juin 2004
38. Schmitt, C.: *Théologie politique*, 1922, rééd. Gallimard (1988)
39. Tugendhat, E.: *Conférences sur l'éthique*, Paris (1998)
40. Velu, J., Ergec, R.: *La Convention européenne des droits de l'homme*. Bruylant, Bruxelles, 1990, no 194
41. Wildt, A.: *Menschenrechte und moralische Rechte*. In: Gosepath, S., Lohmann, G. *Philosophie der Menschenrechte*, Francfort (1998)
42. Zamiatine, E.: *Préface de Jorge Semprun*. In: *Nous Autres*. Gallimard, Paris (1979)

Franck Dumortier
 Published online: 10 February 2009
 © ERA 2009

Biographie sommaire

Franck Dumortier is researcher at the Research Centre for Computer and Law (CRID) of the University of Namur, Belgium, « Freedom in the Information Society » (data protection issues) and « Intellectual property » departments.

In 2004 he graduated in Law at the University of Brussels (ULB), Belgium, cum Laude.

In 2005 he acquired his post-graduate Diploma in Law and Management in Communication and Information Technologies at the University of Namur, Belgium, Magna cum Laude, Eulisp program in Leuven.

He is specialised in the research fields 'Personal Data Protection Legislation' and 'Cybercrime'

Publications importantes

Franck DUMORTIER, Facebook y los riesgos de la "descontextualización" de la información, in IDP, Revista de Internet, Derecho y Política, issue 9, pp. 25-41, 2009

Franck DUMORTIER, L'utilisation de la biométrie et des RFIDs dans le cadre de l'espace européen de liberté, de sécurité et de justice : une affaire de balance ou une question de dignité ? , in ERA Forum, volume 9, issue 4, pp. 543-579, 2008

Franck DUMORTIER, Jean-Philippe MOINY, Jean-Marc VAN GYSEGHEM, Olivia VENET, Olivier HERTMANS, Martin LAURENT, Un badge à l'école, la puce à l'oreille !, in Le Soir, 2007

Franck DUMORTIER, Changes ahead for Israel's DP law, in Privacy laws & Business, issue 86, pp. 6-7, 2007

Franck DUMORTIER, La vidéosurveillance sous l'angle de la proportionnalité : premières réflexions au sujet de la loi réglant l'installation et l'utilisation de caméras de surveillance, in Revue du Droit des Technologies de l'Information, issue 29, pp. 311-350, 2007

Franck DUMORTIER, Michael BIRNHACK, Israel asks EU to assess its DP law for adequacy, in Privacy laws & Business, issue 86, pp. 10-11, 2007

Franck DUMORTIER, Yves POULLET, La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne, in Revue Lamy Droit de l'immatériel, issue 29, pp. 76-86, 2006

Franck DUMORTIER, A propos du sommet mondial sur la société de l'information. Les ambiguïtés de la gouvernance de l'Internet, in Revue du Droit des Technologies de l'Information, issue 25, pp. 143-168, 2006

Franck DUMORTIER, Le fichage et le respect du droit à la vie privée, in L'état des droits de l'homme en Belgique : rapport 2008, pp. 39-50, 2009

Franck DUMORTIER, Caméras de surveillance: la cohabitation légale reste houleuse : à propos du champ d'application de la loi du 21 mars 2007 et de sa coexistence avec d'autres normes réglant les caméras de surveillance, 2009

Yves POULLET, Franck DUMORTIER, La protection des données à caractère personnel dans le contexte de la construction en piliers de l'Union européenne, in Défis du droit à la protection à la vie privée, collection Cahiers du Centre de Recherches Informatique et Droit , volume 31, pp. 447-478, 2006

Mara Verheyden-Hilliard

Brief biography

Mara Verheyden-Hilliard is the co-founder, with Carl Messineo, of the Partnership for Civil Justice, a public interest legal organization in Washington, D.C. that handles constitutional law, civil rights, women's rights, economic justice matters and Freedom of Information Act cases (www.JusticeOnline.org). Her practice includes key constitutional rights litigation, particularly concentrated in the areas of free speech, assembly or other protected political organizing activity. Her work has challenged and exposed government claims of "national security" often used as a pretext for illegal disruption of, and surveillance on, political activities.

She represents political activists and organizations in numerous cases fighting widespread violations of free speech rights, including class action claims arising from mass arrests and brutality at anti-globalization and anti-war demonstrations. Much of PCJ's work has focused on the intersection of First and Fourth Amendment rights -- the right to freedom of speech and the right to be free from illegal police seizure. PCJ's litigation was the first to expose the use of the FBI's Joint Terrorism Task Force against political activists and also revealed that the Washington, D.C. police department maintained a domestic spying operation in which police officers were sent on long-term undercover infiltration assignments posing as members of protest groups to report on political activities, even in the absence of allegations of criminal activity.

She has brought litigation against the government demanding disclosure of documents that reveal improper governmental operations. One such lawsuit is against the Broadcasting Board of Governors, which operates as a propaganda arm of the U.S. government, to force disclosure of payments to journalists who have published false and negative reports in the U.S. media about the Cuban 5 that may have affected their right to a fair trial.

Verheyden-Hilliard has recently won the largest monetary settlements for violations of protestors' rights in U.S. history, totaling 22 million dollars as well as securing extensive changes in both the law and police practices as regards the handling of demonstrations. She has been certified as lead class counsel on behalf of approximately seven hundred class members in *Becker, et al. v. District of Columbia, et al.*, Civil Action No. 01-0811, U.S. District Court for the District of Columbia (alleging false arrest, excessive force and other violations by law enforcement in connection with the April, 2000 IMF/World Bank protests in Washington, D.C., recently settled for \$13.7 million), as lead class counsel on behalf of approximately four hundred class members in *Barham, et al. v. Ramsey, et al.*, Civil Action No. 02-02283, U.S. District Court for the District of Columbia (alleging false arrest in connection with the September, 2002 IMF/World Bank protests in Washington, D.C., recently settled for \$8.25 million); as class counsel with other NLG lawyers

in Killmon, et al. v. City of Miami, et al., Civil Action No. 04-20707, U.S. District Court for the Southern District of Florida (resolving constitutional claims in connection with the 2003 Free Trade of the Americas Act protests).

Among other cases, she has served as lead counsel in Mills, et al v District of Columbia, (obtaining ruling in the U.S. Court of Appeals for the D.C. Circuit finding Washington, D.C.'s seizure and interrogation police checkpoint program to be unconstitutional); Bolger, et al. v. District of Columbia, Civil Action No. 03-906, U.S. District Court for District of Columbia (obtaining settlement in favor of political activists who were targeted and falsely arrest by law enforcement based on political affiliation; obtaining major sanctions against the Attorney General's office for discovery abuse); in A.N.S.W.E.R. Coalition v. Norton, Civil Action No. 05-00071, U.S. District Court for the District of Columbia (successfully enjoining permitting system restricting public attendance along Presidential Inaugural Parade route); in National Council of Arab Americans, et al. v. City of New York, et al, Civil Action 04-6602, U.S. District Court for the Southern District of New York, (successfully challenging the City's efforts to discriminatorily restrict mass assembly in the Great Lawn of Central Park stemming from the Republican National Convention protests of 2004); International Action Center v. City of Philadelphia, Civil Action 01-2217, U.S. District Court for the Eastern District of Pennsylvania (enjoining City's use of protest permitting system and application of youth curfew in the context of free speech activities). Ms. Verheyden-Hilliard obtained a \$5 million judgment at trial in favor of a worker suing for employment based discrimination and retaliation in McCrae v. Daka, D.C. Super. Ct., No. 7505-97 (verdict 2000) which was the largest verdict ever obtained on behalf of an individual claimant in the District of Columbia under the Human Rights Act.

Ms. Verheyden-Hilliard is co-chair of the National Lawyers Guild Mass Defense Committee and serves on the National Executive Committee of the NLG. She is one of the leading voices of the anti-war movement in the United States and in defense of targeted Arab and Muslim communities since September 11, 2001. She is a 1994 graduate of Columbia University Law School and has appeared extensively in the mass media, including on NBC, CBS, ABC, CNN, MSNBC, FOX, C-Span, on NPR, in print media including in the Washington Post and the New York Times as well as in international media.

*Mara Verheyden-Hilliard, Esq.
Partnership for Civil Justice Fund
617 Florida Avenue
Washington, DC 20001 USA
(202) 232-1180
www.JusticeOnline.org*

DE UITWISSELING VAN PERSOONSGEGEVENS IN STRAFZAKEN TUSSEN DE EU-LIDSTATEN EN TUSSEN DE EU EN DE VS

Dr. Els De Busser

Alle EU lidstaten hebben het Raad van Europa Verdrag inzake gegevensbescherming geratificeerd. De EU heeft eigen instrumenten voor gegevensbescherming met betrekking tot de EU instellingen, met betrekking tot telecommunicatie en met betrekking tot strafzaken. Bovendien worden gegevensbeschermingsregels geïntegreerd in verscheidene bilaterale en multilaterale overeenkomsten die de uitwisseling van gegevens omvatten.

En toch is deze regelgeving niet geheel consequent. Bij een nadere studie van het geheel van regels inzake gegevensbescherming blijkt dat de basisprincipes niet volledig worden nageleefd. Het feit dat deze trend niet beperkt wordt tot het domein van de EU lidstaten maar ook wordt doorgezet in de uitwisseling van persoonsgegevens met derde staten, is zorgwekkend. Wanneer het dan ook nog eens gaat om een derde staat die er een bijzonder verscheiden gedachtengoed betreffende gegevensbescherming op na houdt, zoals de VS, dan is het van uiterst groot belang dat de eigen principes gerespecteerd worden. Nochtans blijkt uit de afgesloten akkoorden tussen de EU, Europol en Eurojust enerzijds en de VS anderzijds, dat dit niet het geval is.

De problematiek werd zeer recent opnieuw in de verf gezet door het ijzersterke ‘neen’ dat het Europees Parlement op 11 februari 2010 antwoordde op de vraag naar haar instemming met een nieuw akkoord inzake de uitwisseling van financiële gegevens tussen de EU en de VS. De gegevensbeschermende waarborgen in het akkoord werden – terecht – te zwak bevonden om de in de EU geldende vereisten te vervullen. Dit is de eerste keer dat zulk krachtig signaal wordt gegeven vanuit parlementaire hoek tegen een trend die in een aantal andere instrumenten naar voren werd gebracht. Dankzij het Verdrag van Lissabon heeft het Europees Parlement namelijk de mogelijkheden verkregen om dit soort stappen te ondernemen en de akkoorden met derde staten op de korrel te nemen. Zonder een institutioneel debat te voeren, wordt in deze bijdrage de aandacht gevestigd op het naleven van de eigen gegevens-beschermende normen bij het organiseren van de interne en externe uitwisseling van persoonsgegevens.

De centrale vraag is bijgevolg ‘leeft de EU haar eigen normen na betreffende de bescherming van persoonsgegevens inzake haar gerechtelijke en politieke samenwerking in strafzaken tussen de EU lidstaten en in haar gerechtelijke en politieke samenwerking in strafzaken met de VS?’. Om deze vraag te beantwoorden, wordt in deze bijdrage nagegaan welke normen dienen nageleefd te worden en in hoeverre deze nageleefd worden in de geldende instrumenten in de relaties tussen de lidstaten en in de relaties met de VS.

I. Recht op een privé leven en de bescherming van persoonsgegevens

Het recht op een privé leven – dat sinds het EU Charter voor de rechten van de mens uitdrukkelijk gerelateerd is aan het recht op bescherming van persoonsgegevens - is niet absoluut. Er kan van worden afgeweken, zij het slechts in een beperkt aantal gevallen.

Deze gevallen moeten door de wet zijn toegestaan en noodzakelijk zijn in een democratische samenleving ter vrijwaring van welbepaalde belangen. Het recht op een privé leven kan enkel worden geschonden wanneer deze schending noodzakelijk is om een wettig doel te beschermen. Wettige doeleinden zijn limitatief opgesomd in artikel 8 EVRM: de veiligheid van het land, de openbare veiligheid, het economisch welzijn van het land, de bescherming van de openbare orde en het voorkomen van strafbare feiten, de bescherming van de gezondheid of de goede zeden, of de bescherming van de rechten en vrijheid van anderen.

De legaliteitsvereiste omvat niet alleen de vereiste dat de nationale regel die afwijkt van het recht op privacy in de wet moet worden voorzien, de voorwaarde omvat ook een kwaliteitsnorm. De nationale regelgeving dient namelijk toegankelijk te zijn en dient burgers voldoende te informeren over de gevallen waarin en de wijze waarop hun privacy kan geschonden worden. De privacyschending dient met andere woorden voorzienbaar te zijn, al dient dit te worden beoordeeld op basis van de concrete omstandigheden van de schending in kwestie.

II. EU bescherming van persoonsgegevens in strafzaken in twee richtingen

De EU heeft beschermingsregels voorzien in de rechtsinstrumenten betreffende politieke en justitiële samenwerking in strafzaken. Deze zijn van toepassing op twee types van verkeer van persoonsgegevens.

Ten eerste, wisselen de EU-lidstaten, die onderworpen zijn aan dezelfde principes van gegevensbescherming, persoonsgegevens uit met elkaar.

Ten tweede, kunnen lidstaten persoonsgegevens overdragen aan de politieke of justitiële autoriteiten van derde staten of instellingen die niet noodzakelijk door deze principes gebonden zijn.

De principes werden ontwikkeld door de Raad van Europa in het Verdrag ter bescherming van individuen tegen de automatische verwerking van persoonsgegevens van 1981 (Verdrag inzake Gegevensbescherming). Alle EU-lidstaten zijn gebonden door dit Verdrag. Bovendien werden de gegevensbeschermingsregels uit dit Verdrag geïmplementeerd in de EU rechtsinstrumenten die gegevensbeschermende regels bevatten, zoals de EG richtlijn aangaande gegevensverwerking van 1995 (richtlijn 95/46/EG); de aanbeveling (87)15 van de RvE inzake het gebruik van persoonsgegevens door politiediensten van belang; de Schengen Uitvoeringsovereenkomst, het Europol Besluit, de regels inzake gegevensverwerking van Eurojust, het verdrag van Prüm en het Besluit tot intensivering van grensoverschrijdende samenwerking en ook het recente Kaderbesluit inzake gegevensbescherming in strafzaken. Een studie van deze instrumenten leidt echter tot het besluit dat deze principes niet steeds op consequente en zelfs niet op correcte wijze worden geïmplementeerd in de vermelde instrumenten.

Het 'moederverdrag' van de Raad van Europa omvat twee fundamentele groepen van principes in artikel 5: de principes die de kwaliteit van persoonsgegevens beschermen en deze die de kwaliteit van de verwerking van de persoonsgegevens beschermen.

De kwaliteit van de persoonsgegevens wordt gewaarborgd door te voorzien in correcte gegevens die regelmatig bijgewerkt worden wanneer ze niet meer up-to-date zijn. Bovendien dienen de gegevens geschikt, relevant en proportioneel te zijn in relatie tot het doel waarvoor ze gebruikt worden. Er moet dus een rechtstreeks verband bestaan tussen de verzamelde gegevens en het doel waarvoor ze verzameld werden en gebruikt zullen worden.

Persoonsgegevens moeten eerlijk en rechtmatig verzameld en verwerkt worden. De eerlijke en rechtmatige verwerking wordt volgens het Verdrag inzake Gegevensbescherming gekenmerkt door twee basisprincipes die opnieuw gekoppeld worden aan het doel waarvoor de gegevens gebruikt worden.

Het doelbindingsprincipe schrijft voor dat persoonsgegevens enkel mogen gebruikt worden voor het doel waarvoor ze werden vergaard. Gebruik voor andere doeleinden is slechts toegelaten voor zover dit verenigbaar is met het oorspronkelijke doel.

De onbeperkte bewaring van persoonsgegevens betekent een verhoogd risico op gebruik voor andere doeleinden. Het laatste principe dat artikel 5 van het Verdrag inzake Gegevensbescherming omvat is het principe van beperkte bewaring. Volgens deze regel mogen persoonsgegevens niet langer bewaard worden dan nodig is voor het doel waarvoor ze verzameld werden.

Wanneer persoonsgegevens worden verzonden aan derde staten of internationale instellingen welke niet gebonden zijn door de EU normen inzake gegevensbeschermingen, geldt een bijkomende voorwaarde. De ontvangende staat of instelling dient met name in een passend niveau van gegevensbescherming te voorzien. Deze waarborg werd niet opgenomen in het Verdrag inzake Gegevensbescherming maar in het Aanvullend protocol bij dit verdrag dat dateert van 2001. Dit protocol werd echter slechts door 16 van de 27 lidstaten geratificeerd waardoor de voorwaarde van een passend niveau van gegevensbescherming niet geldt voor alle overdrachten van persoonsgegevens naar een derde staat of instelling.

A. Gegevensverkeer in strafzaken tussen de EU-lidstaten

De kwaliteitsnormen die gelden bij de verwerking van persoonsgegevens, zijn niet ten volle nageleefd in de EU rechtsinstrumenten aangaande politieke en justitiële gegevensuitwisseling in strafzaken.

Het doelbindingsprincipe is weliswaar opgenomen in deze rechtsinstrumenten, de betekenis van het beginsel varieert. Slechts in een beperkt aantal rechtsinstrumenten geldt een strikte doelbinding in dezelfde zin zoals deze opgenomen werd in het Verdrag inzake Gegevensbescherming. De bepalingen in de Schengen Uitvoeringsovereenkomst aangaande wederzijdse rechtshulp, de bepalingen inzake gegevensuitwisseling door Eurojust, het Prüm verdrag en het Besluit tot intensivering van grensoverschrijdende samenwerking zijn de enige instrumenten die het doelbindingsprincipe van de RvE strikt respecteren. Zij laten doelafwending enkel toe voor doeleinden verenigbaar met het doel waarvoor de persoonsgegevens verzameld werden.

In de overige bestudeerde instrumenten wordt systematisch de regel van doelbinding verruimd tot buiten de grenzen van wat een 'verenigbaar' doel kan genoemd worden. Het gebruik van de terminologie 'gebruik voor enig ander doel' verzekert een waaier van mogelijke doeleinden waarvoor de uitgewisselde gegevens mogen gebruikt worden, al dan niet mits toestemming van de verstreckende staat of de betrokkene.

De verbreding van het toegelaten gebruik door middel van deze terminologie is zichtbaar in de EU Rechtshulpovereenkomst van 2000 en in het Kaderbesluit inzake gegevensbescherming in strafzaken van 2008.

Het Kaderbesluit van 2008 inzake gegevensbescherming in strafzaken vormde een ideale opportuniteit om de gegevensuitwisseling in politieke en justitiële samenwerking in strafzaken te voorzien van een sterk apparaat aan gegevensbeschermende waarborgen. Ook dit instrument maakt echter gebruik van de verbreding van het doel waarvoor persoonsgegevens mogen gebruikt worden zonder de noodzakelijkheid daarvan voldoende aan te tonen, wat neerkomt op een niet toegelaten doelafwijking overeenkomstig de bepalingen van het Verdrag inzake Gegevensbescherming.

Hier dient wel te worden opgemerkt dat het Kaderbesluit enkel van toepassing is op de uitwisseling van persoonsgegevens die de lidstaat heeft ontvangen of die haar werden ter beschikking gesteld door een andere lidstaat. De persoonsgegevens die de lidstaat dus zelf verzamelde vallen niet onder het toepassingsgebied van het kaderbesluit, maar worden gereguleerd door nationale bepalingen.

Een breder gebruik van ontvangen persoonsgegevens kan echter nog op twee andere manieren georganiseerd worden.

Ten eerste maken de introductie van het beginsel van beschikbaarheid van gegevens en het aan elkaar verbinden van bestaande databanken – de interoperabiliteit – het gebruik voor andere doeleinden mogelijk. Deze doeleinden zijn niet noodzakelijk verenigbaar met het doel waarvoor de gegevens werden verzameld.

Ten tweede kan de toekenning van nieuwe toegangsrechten tot bestaande informatiesystemen voor bepaalde autoriteiten, zoals de toegangsrechten van Europol en Euro-just tot het Schengen Informatiesysteem (SIS II) zorgen voor een doelafwijking van de bestaande gegevens.

De verscheidene mogelijkheden die in de bestudeerde rechtsinstrumenten worden geboden om af te wijken van het oorspronkelijke doel waarvoor persoonsgegevens werden verzameld, stroken niet met de voorgeschreven normen inzake gegevensbescherming door de RvE. De ratio legis van het doelbindingsprincipe is immers dat de doeleinden waarvoor de uitgewisselde informatie mag gebruikt worden, beperkt zijn. Bovendien is de afwijking van de norm niet in elk geval gerechtvaardigd door de noodzakelijkheidsvereiste.

Het besluit is bijgevolg dat de bepalingen van de EU rechtsinstrumenten inzake politieke en justitiële gegevensuitwisseling tussen de lidstaten, inclusief de uitwisseling met Europol en Eurojust, niet volledig in overeenstemming zijn met de normen neergelegd in het Verdrag inzake Gegevensbescherming.

Een gelijkaardige evolutie is zichtbaar op het vlak van de norm inzake de beperkte bewaring van persoonsgegevens of data retentie. Het bewaren van persoonsgegevens in een bestand voor een langere

periode dan nodig is voor het doel waarvoor ze verzameld werden, strookt niet met de norm uit artikel 5 van het Verdrag inzake Gegevensbescherming. De richtlijn inzake data retentie voor strafrechtelijke doeleinden omvat echter een verplichting in hoofde van telecommunicatieondernemingen om persoonsgegevens te bewaren voor mogelijk later gebruik in strafzaken. Het gaat hier dus niet alleen om een onverenigbaar doel in vergelijking met het oorspronkelijk doel, de noodzaak van deze bewaring – vereist overeenkomstig het Verdrag inzake Gegevensbescherming om een uitzondering te maken op de normen uit artikel 5 – blijft onduidelijk.

Ook op het vlak van de beperkte bewaring van gegevens zijn de bepalingen in de EU rechtsinstrumenten dus niet volledig in overeenstemming met de voorgeschreven normen.

B. Gegevensverkeer in strafzaken tussen EU-lidstaten en een derde staat of instelling

De uitwisseling van persoonsgegevens naar derde staten of instellingen betekent een mogelijke onderwerping aan andere gegevensbeschermingsregels. Om de eigen gegevensbescherming te waarborgen, voerde de RvE de voorwaarde in van een passend niveau van gegevensbescherming. De ontvangende staat of instelling dient m.a.w. over een regelgeving te beschikken die de te verstrekken persoonsgegevens een bescherming biedt die geschikt is in vergelijking met de bescherming geboden door de EU normen inzake gegevensbescherming.

Deze voorwaarde is echter geen algemene voorwaarde voor alle gegevensstromen uitgaande van een EU lidstaat.

In de eerste plaats hebben niet alle lidstaten het Aanvullend Protocol bij het Verdrag inzake Gegevensbescherming geratificeerd. Het Kaderbesluit inzake gegevensbescherming in strafzaken omvat de voorwaarde van een passend niveau van gegevensbescherming, maar is enkel van toepassing op gegevens verkregen of ter beschikking gesteld door een andere lidstaat. Voor gegevens verzameld door de verstreckende lidstaat geldt de voorwaarde dus niet, tenzij deze staat gebonden is door het vermelde Protocol.

Bovendien voorziet het Kaderbesluit in een aantal belangrijke uitzonderingen op de voorwaarde van een passend niveau van gegevensbescherming. Gerechtvaardigde, doorslaggevende belangen, met name zwaarwegende openbare belangen, laten toe van deze vereiste af te wijken. Aangezien de strafrechtelijke vervolging van misdrijven als een gerechtvaardigd en doorslaggevend belang wordt gezien door de RvE, wordt de voorwaarde van een passend niveau van gegevensbescherming uitgehold.

Een bijkomend vraagstuk is de invulling van de vereiste. Ondanks de bezorgdheid van de Europese Toezichthouder voor Gegevensbescherming, bestaat geen uniforme regeling omtrent de manier waarop een gegevensbeschermingssysteem dient te worden 'getest' op haar adequaat karakter. Wanneer de doorgifte van persoonsgegevens door Europol en Eurojust naar derde staten of instellingen onder de loep wordt genomen, zien we ook daar grote verschillen. Europol beschikt over een trapsgewijs controlesysteem alvorens de doorgifte wordt toegelaten, terwijl Eurojust enkel vertrouwd op haar eigen gegevensbeschermingsbeambte zonder de Raad in te schakelen.

Een behoorlijke bescherming van persoonsgegevens in de strafrechtelijke samenwerking met derde staten of instellingen zou dus wel varen bij een algemeen geldende vereiste die tevens een uniforme invulling krijgt om misbruiken of 'data shopping' tegen te gaan.

III. Samenwerking EU – VS in strafzaken

A. Gegevensbescherming in de VS

Vooraleer de samenwerking tussen de EU en de VS in strafzaken kan bestudeerd en beoordeeld worden, dienen de Amerikaanse regels op gegevensbescherming te worden onderzocht. Van een ware spiegelstudie kan echter geen sprake zijn vermits het model van gegevensbescherming dat de VS heeft ontwikkeld fundamenteel verschillend is van het EU model. Deze laatste voorziet – zoals hoger aangegeven – in een algemeen kader van normen inzake gegevensbescherming door middel van het RvE Verdrag inzake Gegevensbescherming en de EU instrumenten. In de VS daarentegen is geen algemeen kader voorhanden maar een combinatie van sectorspecifieke reguleringen, zelfregulering door ondernemingen en technologieën met gegevensbeschermende functie. Het dichtst bij een algemene bepaling is het Vierde Amendement bij de Amerikaanse Grondwet. Deze bepaling legt voorwaarden neer bij het betreden van privé terrein, het in beslag nemen van goederen en gegevens en het arresteren van personen. Het gaat echter om een grondregel die onvoldoende gedetailleerd of uitgebreid is – en bovendien onderhevig aan de interpretatie van het Amerikaanse Hooggerechtshof – om in een passend wetgevend kader van gegevensbescherming te voorzien.

In de jaren '70 werd een geheel van niet-bindende principes ontwikkeld door het Amerikaanse Ministerie van gezondheid, opvoeding en welzijn – de Fair Information Practice principles – dat beginselen omvat die bijzonder dicht bij het Verdrag inzake Gegevensbescherming liggen. Bovendien is de VS lid van de OECD en APEC, twee samenwerkingsverbanden die ook een geheel van niet-bindende beginselen inzake gegevensbescherming ondersteunen die sterk aanleunen bij de door de RvE voorgescreven normen. Toch is de implementatie van de principes niet gelijklopend in de EU en de VS.

De betekenis van de gebruikte basistermen in de EU en de VS – privacy en persoonsgegevens – zijn voldoende in overeenstemming met elkaar.

De bindende normen die gelden op gegevensuitwisseling in strafzaken in de VS geven echter een ander plaatje.

Het doelbindingsprincipe als algemeen beginsel kent geen equivalent in de Amerikaanse gegevensbescherming. Specifieke regels op het gebruik van persoonsgegevens zijn weliswaar van kracht (bv. bij het huren van video's) maar het toegelaten gebruik van persoonsgegevens steunt op een redenering die het omgekeerde is van de EU redenering.

Terwijl in de EU de algemene regel de gebruiksbepierking tot verenigbare doeleinden omvat tenzij de toestemming van de betrokkene wordt verkregen, vertrekt men in de VS van de algemene regel dat het gebruik van persoonsgegevens slechts is toegelaten mits de toestemming van de betrokkene met als uitzondering het gebruik voor routine doeleinden. Dit betekent dat gebruik voor verenigbare doeleinden

zonder toestemming de algemene regel vormt in de EU maar de uitzondering is in de VS. Hierbij dient evenwel te worden vermeld dat de zogenaamde 'routine uses' zodanig vaak aangewend worden dat ze in de praktijk eerder de regel vormen dan de uitzondering.

Net zoals de EU rechtsinstrumenten voorziet de Amerikaanse wetgeving in de doelafwending van persoonsgegevens. De manier waarop deze doelafwending wordt georganiseerd is echter uiteenlopend. Terwijl de EU rechtsinstrumenten toelaten dat persoonsgegevens worden gebruikt voor een ander doel nadat ze werden verzameld in overeenstemming met de gegevensbeschermingswetgeving, wordt in de Amerikaanse wetgeving de standaard van gegevensbescherming reeds verlaagd bij het verzamelen van de gegevens. Administratieve autoriteiten hebben in de VS namelijk brede opsporingsbevoegdheden en kunnen krachtens wetten die voornamelijk na 11 september 2001 werden afgekondigd, vaak persoonsgegevens verwerven door middel van privacyschendende technieken. Voorbeelden hiervan zijn de FISA mandaten die autoriteiten toelaten buiten het Vierde Amendement om, persoonsgegevens te verzamelen en later te gebruiken in strafzaken.

Een algemene regel op de beperkte bewaring van persoonsgegevens bestaat niet in de VS. Slechts summiere bepalingen in specifieke wetgeving, bijvoorbeeld op het bewaren van gegevens van de verhuur van video's, voorzien in een maximum bewaartijd.

Vanuit het oogpunt van de EU kan dus niet geconcludeerd worden dat de VS over een passend niveau van gegevensbescherming beschikt. Beide systemen zijn niet verenigbaar met elkaar zonder de garantie van bijkomende beschermingswaarborgen. In het volgende deel zal echter blijken dat de vereiste van een passend niveau van gegevensbescherming niet consequent wordt toegepast en dus geen bescherming biedt tegen afwijkende regels in derde staten of instellingen.

B. Overeenkomsten EU – VS in strafzaken

1. Doelbinding en passend niveau van gegevensbescherming

De uitwisseling van persoonsgegevens in strafzaken tussen EU lidstaten en de VS werd traditioneel gereguleerd door bilaterale overeenkomsten of MLATs (mutual legal assistance treaties) en enkele multilaterale overeenkomsten. Deze zijn hoofdzakelijk op justitiële samenwerking gericht. Op het vlak van wetshandhaving was het Europol dat een eerste akkoord sloot met de VS na de gebeurtenissen van 11 september 2001 aangaande de uitwisseling van strategische en technische informatie. Een tweede akkoord over de uitwisseling van persoonsgegevens volgde in 2002.

Twee elementen zijn bijzonder opvallend aan dit tweede akkoord. Ten eerste is het akkoord aangevuld met een reeks informele nota's. Deze bevatten echter informatie die cruciaal is om de juiste draagwijdte van de verbintenissen uit het akkoord te begrijpen. De uitbreiding houdt immers een duidelijk doelafwending in aangezien gegevens buiten strafzaken kunnen gebruikt worden.

Bovendien vormt het geheel van federale en lokale wetshandhavingsdiensten in de VS een bijzonder complexe partner. Europol heeft daarop kunnen bewerkstelligen dat de lokale autoriteiten zich uitdrukkelijk moeten gebonden verklaren door de bepalingen van het akkoord.

Ten tweede laat het akkoord tevens niet toe dat de vereiste van een passend niveau van gegevensbescherming in hoofde van de VS wordt gesteld. M.a.w. Europol heeft er tijdens de onderhandelingen met de VS mee ingestemd om haar eigen regels inzake gegevensbescherming bij uitwisseling met derde staten, niet na te leven.

De verbreding van het doel waarvoor persoonsgegevens mogen gebruikt worden is eveneens zichtbaar in de EU – VS rechtshulpovereenkomst van 2003; het Eurojust – VS akkoord van 2006 en het in 2010 aan het Europees Parlement voorgestelde ontwerp akkoord aangaande de overdracht van financiële gegevens.

De EU – VS overeenkomst inzake rechtshulp in strafzaken is een apart voorbeeld van de transatlantische relaties aangezien dit de eerste overeenkomst is – samen met de overeenkomst inzake uitlevering van dezelfde datum – gebaseerd op de combinatie van artikel 24 en artikel 38 van het VEU. Dit is de eerste keer dat de EU als gelijke partner tegenover de VS stond in de onderhandelingen. De rechtshulpovereenkomst is op 1 februari 2010 in werking getreden. Elke lidstaat heeft bovendien een bilateraal instrument aangenomen dat de toepassing van de overeenkomst interpreteert. Opvallend is dat de specialiteitsregel die traditioneel in elke bilaterale MLAT vervat was, vervangen wordt door het doelbindingsprincipe, zij het in een versie waarbij het gebruik voor enig ander doel is toegelaten met de toestemming van de verstreckende staat of de betrokkene.

Dit bevestigt de trend van doelafwending die hoger reeds werd aangetoond in de EU rechtsinstrumenten aangaande politieke en justitiële gegevensuitwisseling tussen de lidstaten.

Het doelbindingsprincipe heeft dan ook een andere draagwijdte in de relaties met de VS die sterk afwijkt van de betekenis die aan het beginsel wordt gehecht in de EU. Deze geformaliseerde doelafwending wordt immers versterkt door de praktijk van ‘data sharing’ tussen de Amerikaanse autoriteiten en de onduidelijke inhoud van het begrip ‘wetshandhavingsdiensten’ in de VS. Ofschoon de High Level Contact Group – bestaande uit vertegenwoordigers van de Europese Commissie, het EU voorzitterschap en vertegenwoordigers van de Amerikaanse ministeries van justitie, binnenlandse zaken en veiligheid van de staat – in 2008 trachtte enkele gemeenschappelijke beginselen te definiëren, werd de betekenis van deze term niet nader toegelicht.

Doelafwending bij het gebruik van persoonsgegevens door de Amerikaanse autoriteiten is tijdens de voorbije jaren in twee zaken bijzonder duidelijk naar voren gebracht. Persoonsgegevens die in de EU voor commerciële doeleinden worden verzameld en vervolgens op vraag van Amerikaanse administratieve autoriteiten worden doorgegeven en verwerkt in de strijd tegen terrorisme en de financiering van terrorisme, was de kernproblematiek in de zogenaamde PNR-zaak (Passenger Name Records) en de SWIFT-zaak. In beide zaken kwamen de relevante Amerikaanse autoriteiten (in het geval van de passagiersgegevens ging het om het Bureau for Customs and Border Protection en in het geval van SWIFT om de United States Treasury) met de bevoegde Europese autoriteiten overeen om engagementen aan te gaan omtrent de bescherming van de ontvangen gegevens. Opnieuw was het doorgeven van deze gegevens aan andere Amerikaanse autoriteiten een mogelijkheid in de PNR-zaak. De EU ging hier akkoord met de verbintenis om de gegevens door te geven aan autoriteiten die bevoegd zijn voor aan openbare veiligheid gerelateerde zaken, zonder dat duidelijk werd aangetoond waarom deze data sharing noodzakelijk was.

Ook in de SWIFT-zaak ging de EG akkoord met een transfer van persoonsgegevens naar de United States Treasury met als voorwaarde dat een specifieke doelbindingsregel het gebruik van de gegevens beperkt tot onderzoeken naar terrorisme financiering en de vervolging daarvan. In dit geval waren bovendien de lange bewaartijden voor de verzamelde gegevens een bijkomend probleem. Niettemin kunnen de geboden waarborgen niet verhinderen dat in de toekomst de United States Treasury verder gebruik zal maken van administratieve bevelen om persoonsgegevens op te eisen van SWIFT.

De voorbije maanden werden onderhandelingen gevoerd om deze overdracht van gegevens in een tijdelijk akkoord te gieten met de intentie om de onderhandelingen verder te zetten in functie van een permanente overeenkomst voor de overdracht van financiële gegevens.

Door de inwerkingtreding van het Verdrag van Lissabon Verdrag op 1 december 2009, werd de nieuwe regelgeving met betrekking tot het Europees Parlement van toepassing. Deze nieuwe regelgeving (gebaseerd op de combinatie van artikel 218, 6, a); artikel 82, 1, d) en artikel 87, 2, a) van het Geconsolideerd Verdrag inzake de Werking van de EU) betekent dat voor akkoorden met derde staten inzake aangelegenheden waarvoor de gewone wetgevingsprocedure geldt, de goedkeuring van het Parlement moet verkregen worden.

Ondanks de druk vanuit Amerikaanse hoek om dit akkoord in werking te laten treden, bleken de frustraties van het Parlement omtrent de tekst zich op te stapelen.

In de eerste plaats hekelde het Parlement het gebrek aan voldoende tijd om de tekst van het akkoord deftig te bestuderen. De tijd die het kostte om de tekst te vertalen leidde ertoe dat het EP de tekst pas op 25 januari ontving terwijl de overeenkomst voorzien was in werking te treden op 1 februari.

Begin februari werd in het Committee on Civil Liberties, Justice and Home Affairs rapporteur Jeanine Hennis-Plasschaert aangeduid om een aanbeveling voor te bereiden betreffende de stemming. Het rapport bevat gelijkaardige argumenten zoals hoger aangegeven. De gegevensbeschermende waarborgen die gelden in de EU werden in het akkoord niet volledig nageleefd.

Meer nog, het tijdelijke akkoord blijkt in hetzelfde bedje ziek als de hoger vermelde Europol, Eurojust en EU akkoorden met de VS. Opnieuw wordt de vereiste van een passend niveau van gegevensbescherming verondersteld in plaats van onderzocht.

Het negatieve rapport werd vertaald in een aanbeveling van het Committee het SWIFT-akkoord te verwerpen. Met een duidelijke meerderheid (378 stemmen tegen, 196 voor en 31 onthoudingen) volgde het Europees Parlement op 11 februari deze aanbeveling. In een laatste poging om de parlementsleden te overtuigen het akkoord niettemin goed te keuren, maakten de lidstaten belangrijke beloftes om het Parlement meer te betrekken bij de onderhandelingen van het reeds geplande permanente SWIFT-akkoord. Dit verhaal wordt ongetwijfeld vervolgd.

2. Bewaring van persoonsgegevens

Wat betreft de beperkte bewaring van persoonsgegevens, gaat Amerikaanse wetgeving uit van een algemene bewaring van persoonsgegevens. Dit betekent een gebrek aan een equivalent van het beginsel van beperkte bewaring zoals dat voorgeschreven werd door de RvE. Dit leidde in de PNR-zaak tot een

initiële bewaartijd van vijftig jaar die na onderhandeling werd teruggedrongen tot vijftien jaar. De EU kon niet vermijden dat een nieuw begrip werd ingevoegd in de meest recente overeenkomst aangaande de doorgifte van passagiersgegevens, met name de 'dormant data' of 'slapende gegevens' die eerder beperkt worden op het vlak van hun toegangsrechten dan op het vlak van hun bewaartijd.

Vervolgens zorgt de Amerikaanse praktijk van data sharing in combinatie met de lange bewaartijd van gegevens voor een situatie van onzekerheid. De bewaartijd van de gegevens is immers afhankelijk van de ontvangende autoriteit, waardoor de verstrekende partij in de EU geen zicht heeft op het lot van de door haar verstrekte gegevens.

IV. Conclusies

De normen die gelden in de EU inzake gegevensbescherming in strafzaken worden niet volledig nageleefd in de rechtsinstrumenten die de uitwisseling van persoonsgegevens voorzien tussen de EU lidstaten. Het uitbreiden van de doeleinden waarvoor ontvangen gegevens mogen gebruikt worden gaat niet samen met de ratio legis van het doelbindingsbeginsel dat verplicht het gebruik van persoonsgegevens te beperken tot doeleinden die verenigbaar zijn met het doel waarvoor de gegevens verzameld werden.

Ook de beperkte bewaring van de verzamelde persoonsgegevens wordt als beginsel miskend in de EU rechtsinstrumenten betreffende gegevensuitwisseling voor strafrechtelijke doeleinden. De richtlijn inzake data retentie laat een algemene bewaring van gegevens toe voor een potentieel gebruik in strafzaken en kan niet gerechtvaardigd worden door de toegelaten uitzonderingen in het Verdrag inzake Gegevensbescherming.

Bovendien is het frappant dat de EU nog steeds geen werk heeft gemaakt van een algemeen rechtsinstrument voor de uitwisseling van persoonsgegevens door wetshandhavingdiensten. Terwijl de justitiële uitwisseling kan rekenen op een aantal regelgevende kaders, dient de politieke uitwisseling van persoonsgegevens terug te vallen op nationale bepalingen. Het Kaderbesluit van 2008 omvat immers enkel de gegevens die werden doorgegeven of ter beschikking gesteld door een andere lid-staat.

In de relaties met de VS worden deze inconsistenties verder versterkt. Het ontbreken van een instrument inzake politieke uitwisseling laat zich ook hier voelen en wordt sterk in de verf gezet door de moeilijkheden die het VS politielandschap met zich meebrengen.

Opmerkelijk is het terzijde schuiven van de vereiste van een passend niveau van gegevensbescherming. Eerder dan het niveau van gegevensbescherming van de VS grondig te onderzoeken, wordt bijzonder snel de adequaat-stempel gezet op de transatlantische samenwerking in strafzaken. A fortiori wordt de vereiste van de onderhandelingstafel geveegd.

De recente gebeurtenissen omtrent het geplande SWIFT-akkoord scheppen de hoop dat het nieuw te onderhandelen akkoord aangaande de overdracht van SWIFT-gegevens kan tegemoet komen aan deze bekommernissen, niet in het minst door de sterkere betrokkenheid van het Europees Parlement.

Niettemin toont onderzoek aan dat de VS als partner in de uitwisseling van persoonsgegevens in strafzaken fundamenteel te verschillend is om met de EU gegevens uit te wisselen zonder bijkomende waarborgen te stellen. Het is echter gebleken dat ook de reeds geponeerde bijkomende waarborgen zoals de vereiste van een passend niveau van gegevensbescherming in strafzaken, het gebruik van persoonsgegevens voor onverenigbare doeleinden niet kan tegenhouden.

Bibliografie

Verdrag ter bescherming van individuen tegen de automatische verwerking van persoonsgegevens, ETS nr. 108, 28 januari 1981.

Comité van Ministers, Aanbeveling nr. R (87) 15 aan de lidstaten betreffende het gebruik van persoonsgegevens in de politieke sector, 17 september 1987.

Europees Parlement en Raad, Richtlijn nr. 95/46/EG, 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, P.B. L 281, 23 november 1995, p. 31-50.

Overeenkomst 29 mei 2000 betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, P.B. C 197, 12 juli 2000, p. 1-23.

Aanvullend Protocol bij het Verdrag ter bescherming van individuen tegen de automatische verwerking van persoonsgegevens aangaande toezichthoudende autoriteiten en grensoverschrijdende gegevensuitwisseling, ETS nr. 181, 8 november 2001.

Overeenkomst tussen de Verenigde Staten en Europol, 6 december 2001 (Europol-US overeenkomst), www.europol.europa.eu

Overeenkomst 25 juni 2003 aangaande rechtshulp tussen de Europese Unie en de Verenigde Staten, P.B. L 181, 19 juli 2003, p. 34-42.

Overeenkomst tussen Eurojust en de Verenigde Staten, 6 november 2006, www.eurojust.europa.eu.

Verdrag van Lissabon 13 december 2007 tot wijziging van het Verdrag betreffende de Europese Unie en het Verdrag tot oprichting van de Europese Gemeenschap, P.B. C 306, 17 december 2007, p. 1-231.

Brief van het ministerie van Financiën van de Verenigde Staten over SWIFT/Programma voor het opsporen van de financiering van terroristische activiteiten; Verwerking van uit de EU afkomstige persoonsgegevens door het Amerikaanse ministerie van financiën ten behoeve van terrorismebestrijding — „SWIFT” en Antwoord van de Europese Unie aan het ministerie van Financiën van de Verenigde Staten — SWIFT/Programma voor het opsporen van de financiering van terroristische activiteiten, P.B. C 166, 20 juli 2007, p. 17-27.

Overeenkomst 23 juli 2007 tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en overdracht van persoonsgegevens van passagiers (PNR-gegevens) door luchtvaartmaatschappijen aan het ministerie van Binnenlandse veiligheid van de Verenigde Staten van Amerika (PNR-overeenkomst 2007), P.B. L 204, 4 augustus 2007, p. 18.

Raad, 9831/08, EU US Summit, 12 juni 2008 – Eindrapport van de EU-US High Level Contact Group met betrekking tot informatie uitwisseling en privacy en gegevensbescherming, 28 mei 2008.

Raad, Kaderbesluit 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politieke en justitiële samenwerking in strafzaken, P.B. L 350, 30 december 2008, p. 60-71.

Besluit van de Raad betreffende de ondertekening, namens de Europese Unie, van de overeenkomst tussen de Europese Unie en de Verenigde Staten van Amerika inzake de verwerking en de doorgifte van gegevens betreffende het betalingsberichtenverkeer van de Europese Unie aan de Verenigde Staten ten behoeve van het Programma voor het traceren van terrorismefinanciering, 16110/09, 27 november 2009.

Beknopte biografie

Dr. Els De Busser is Licenciaat Rechten, vervulde een Aanvullende Opleiding in de Criminologie en behaalde een Master na Master's Degree in European Criminology and Criminal Justice Systems. Van maart 2001 tot oktober 2009 was zij werkzaam als wetenschappelijk onderzoekster en vervolgens assistente aan de Universiteit Gent, Vakgroep Strafrecht en Criminologie, Onderzoeksgroep IRCP (Institute for International Research on Criminal Policy). Daar verleende zij assistentie bij de vakken Internationaal Strafrecht, Strafrecht, Europese en Internationale Instellingen en Organisaties en European Criminal Policy en specialiseerde zij zich in het Europees strafrecht.

Aan de Universiteit Gent verdedigde zij haar doctoraat in 2009 met een proefschrift met als titel 'EU internal and transatlantic cooperation in criminal matters from a personal data perspective. A substantive law approach'. In dit proefschrift bestudeerde Dr. De Busser de geldende gegevensbeschermingsregels in de gerechtelijke en politieke samenwerking in strafzaken tussen de EU lidstaten en in de samenwerking tussen de EU en de VS.

Sinds november 2009 is zij werkzaam als senior researcher in de afdeling Europäisches Strafrecht / European Criminal Law aan het Max-Planck-Institut für ausländisches und internationales Strafrecht te Freiburg, Duitsland.

Haar publicaties omvatten o.a. volgende boeken en artikelen:

- Els De Busser, 'EU data protection in transatlantic cooperation in criminal matters: will the EU be serving its citizens an American meal?', *Utrecht Law Review*, Vol. 6, 1, 2010, p. 86-100;
- Els De Busser en Gert Vermeulen, 'Towards a coherent EU policy on outgoing data transfers for use in criminal matters? The adequacy requirement and the framework decision on dataprotection in criminal matters. A transatlantic exercise in adequacy', in *Topical Issues in EU and International Crime Control*, Antwerp-Apeldoorn, Maklu, 2010, p. 93 – 120;
- Els De Busser, *Data Protection in EU and US Criminal Cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Antwerp-Apeldoorn, Maklu, 2009, 473p.;
- Els De Busser, 'Purpose limitation in EU-US data exchange in criminal matters: the remains of the day', in Marc Cools et.al., *Readings on Criminal Justice Criminal Law & Policing*, GOFS Research Paper Series, Antwerp-Apeldoorn, Maklu, 2009, p. 163-201;
- Els De Busser, *Judicial cooperation in criminal matters: mutual legal assistance*, in Conny Rijken and Gert Vermeulen, *Joint Investigation Teams in the European Union, from theory to practice*, 2006, TMC Asser Press, the Hague, p. 119 – 158.

UTILITÉ ET FUTILITÉ DES RECOURS EN MATIÈRE DE FICHAGE PAR LES SERVICES RÉPRESSIFS.

Mathieu Beys¹

«La garantie des droits de l'Homme et du Citoyen nécessite une force publique: cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée.»

(article 12 de la Déclaration des droits de l'homme et du citoyen de 1789²)

Introduction

«L'intéressé est également connu de nos services pour des faits de... (au choix: tapage nocturne, stupéfiant, prostitution, vol à la tire)». Les avocats pénalistes sont confrontés régulièrement à ce type de mention sibylline figurant dans un procès-verbal, même lorsque le casier judiciaire de leur client est blanc comme neige. Le « déjà connu de nos services » revient comme une ritournelle dans la rhétorique policière, comme une sorte de label destiné à rendre plus crédibles les accusations présentes alors qu'il n'est souvent étayé par aucun élément concret. C'est le pouvoir du fichage policier: faire ressortir au bon moment une information, même si celle-ci n'a aucun rapport avec l'affaire en cours. Elle donnera un pedigree au prévenu et le juge pourra y être sensible, au moins inconsciemment.

Dans la poursuite des crimes et délits (mission de police judiciaire) et la prévention des atteintes à l'ordre public (mission de police administrative), le travail policier est évidemment inconcevable sans la récolte et le traitement d'informations sensibles. Mais pour les services répressifs plus que chez le commun des mortels « l'information, c'est le pouvoir ». L'appétit policier pour l'information a donc une tendance naturelle à devenir gargantuesque. Depuis belle lurette³, le fichage répressif et les droits individuels ont entretenu des relations conflictuelles. Mais plusieurs facteurs sont venus renforcer cette tension ces derniers temps: mélange des genres entre police et renseignement⁴, mise en place de bases de données dans le cadre de l'Union

¹ L'auteur remercie toutes les personnes qui l'ont aidé pour la préparation de cet article et tout particulièrement Axel Bernard. Il reste évidemment seul responsable des éventuelles approximations et imperfections du contenu.

² Texte intégral disponible sur: <http://www.assemblee-nationale.fr/histoire/dudh/1789.asp>

³ Nommé ministre de la guerre en France en 1900, le général André fait établir près de 25 000 fiches sur les opinions politiques et religieuses d'officiers afin de républicaniser l'état-major des armées. On peut y lire par exemple « VLM » pour « va à la messe », « grand avaleur de bon Dieu », « rallié à la République, n'en porte pas moins un nom à particule », « a qualifié les maçons et les républicains de canailles, de voleurs et de traîtres », « vit maritalement avec une femme arabe » ou encore « vieille peau fermée à nos idées ». Dès la révélation de l'existence de ces fiches, en 1904, le général André est contraint de démissionner (Assemblée nationale, Rapport d'information n° 1548 sur les fichiers de police, déposé par Delphine BATHO et Alain BENISTI, 24 mars 2009, p 12.)

⁴ Les fichiers de renseignement ne font pas l'objet de la présente contribution. Sur les craintes concernant le projet de loi sur les méthodes particulières de renseignement voir notamment Tom DECAIGNY, Paul DE HERT, « De Wet bijzondere methoden inlichtingen- en veiligheidsdiensten (BIM) », Ad Rem, 1/2009, pp. 24-35. Une version amendée du projet a été adoptée par le Sénat le 21 janvier 2010. Voir le doc. Parl. Ch. N° 52 / 2128 sur le site www.lachambre.be.

européenne⁵, échanges croissants d'informations sur le plan international...Le propos de la présente contribution se limite aux fichiers des services policiers en Belgique et aborde brièvement la question de cette tension dans une perspective résolument pratique. Une forme de contrôle démocratique ou citoyen sur les fichiers policiers relève-t-elle de l'idée saugrenue? Certains épisodes des annales policières récentes nous montreront qu'il n'en est rien (I). Les mécanismes d'information et de recours du citoyen existant à l'heure actuelle à l'égard de ses données personnelles ne paraissent pas particulièrement convaincants (II). On est en droit de se poser des questions sur la compatibilité de ces faibles gardes-fous avec les normes supérieures protégeant notamment la vie privée telle la Convention européenne des droits de l'homme (III).

I. Un droit de regard citoyen sur les fichiers policiers: idée subversive ou nécessité démocratique?

Plusieurs phénomènes, anciens ou plus récents, observés sur la scène belge, européenne ou internationale illustrent la nécessité d'un droit de regard sur les fichiers policiers. On se contente ici d'en passer quelques uns en revue.

I. 1. Profilage ethnique: juste quelques « dérapages » ou tendance lourde?

Au milieu des années 90, inspirée par des méthodes de pays voisins⁶, la gendarmerie a mis en place une curieuse opération baptisée « Rebel », visant exclusivement les organisations criminelles « turques », avec l'objectif d' « identifier les vrais responsables du trafic d'héroïne en Belgique ». En 1996, la presse avait fait le lien entre ce fichage massif de ressortissants turcs et de Belges d'origine turque et un accord de collaboration entre la gendarmerie belge et le ministère de l'intérieur turc. Devant le parlement, l'explication du ministre de la justice de l'époque est tout sauf convaincante: il s'agissait de ficher certains membres de la communauté turque pour parvenir à identifier des « caïds » de la drogue, sachant que le marché de l'héroïne en Belgique était notamment au main du milieu turc. Un sénateur ironise: Va-t-on commander un screening de tous les Ovest Flamands si on remarque que beaucoup d'auteurs de fraudes dans le secteur du textile et des trafiquants d'hormones sont originaires de Flandre occidentale?⁷. Le Comité P, organe de contrôle des services de police, est chargé d'enquêter sur cette affaire. Il faudra attendre 5 ans pour obtenir... la même explication, à peu de choses près. Il s'agissait donc de partir de la « communauté » en récoltant les données personnelles de 90 330 personnes, qui ont ensuite fait l'objet d'un traitement dépersonnalisé permettant d'obtenir une idée de plusieurs éléments « sociodémographiques » concernant la communauté turque de Belgique : présence par région, localisation de grands groupes de population, pyramide des âges... Sur base de ces informations, la gendarmerie aurait identifié des « criminels potentiels » (5 185 personnes qui, après une sélection basée sur les profils, a été ramenée à 61 personnes sur base de critères élaborés en fonction des analyses de profil de criminels notoires). Selon le Comité P, aucune illégalité n'a été commise et l'opération se justifiait par l'objectif de « parvenir à identifier les vrais

⁵ Le meilleur exemple est le Système d'information Schengen (SIS), d'abord consacré essentiellement à la lutte contre l'entrée des étrangers indésirables dans l'espace du même nom, il s'est élargi pour devenir un outil de contrôle visant aussi les citoyens européens (SIS II). Voir à ce sujet l'impressionnante thèse d'Evelien BROUWER, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Leiden/Boston: Martinus Nijhoff Publishers, series Immigration and Asylum Law and Policy in Europe, 2008.

⁶ Angleterre (Centurionproject), Pays-Bas (IRT) et Allemagne (Anadalou), selon le Rapport annuel 2001 du Comité P, p 40, www.comitep.be.

⁷ Voir notamment les interventions des sénateurs Boutmans et Erdman, Doc. Parl., Sénat, 1995-1996, *Annales de la réunion publique de commission*, réunion de la commission de la justice du 3 juillet 1996, pp.303-312 et *Compte rendu analytique* du 3 juillet 1996, Sénat, réunions publiques de commission, pp.202-206.

responsables du trafic d'héroïne en Belgique »⁸. Malheureusement, les questions de départ sont restées sans réponses: en quoi était-il nécessaire de récolter des données personnelles sur plus de 90.000 personnes pour identifier quelques dizaines de criminels potentiels? Pourquoi ne pas concentrer l'attention sur les milieux déjà identifiés ? A-t-on pu vérifier que l'analyse des données sur ces 90.000 personnes a bien été « dépersonnalisée » et ne contenait que des éléments « sociodémographiques » ? Et enfin, combien de « caïds » a-t-on pu identifier, et faire condamner grâce à l'opération « Rebel »? On n'en sait toujours rien à l'heure actuelle. Mais, pour le Comité P, aucune raison de s'inquiéter, et, d'ailleurs, « des projets de ce type sont actuellement presque monnaie courante »⁹.

Depuis lors, les opérations de « profilage ethnique » ont effectivement le vent en poupe dans de nombreux pays engagés dans la lutte contre le terrorisme. Entre 2001 et 2003, la police allemande a recueilli des données sensibles d'environ 8,3 millions de personnes aux profils similaires à ceux de la cellule de Hambourg, dont certains auteurs des attentats du 11 septembre 2001 faisaient partie. Une base de données d'environ 32.000 terroristes dormants potentiels a été établie: des hommes entre 18 et 40 ans, (ex)étudiants, musulmans ou originaires d'un pays où l'islam est majoritaire. Suite à la collecte et au recoupement de très nombreuses autres données notamment auprès d'universités, d'institutions de sécurité sociale, d'autorités locales, les policiers se focaliseront finalement sur 1.689 personnes. Celles-ci feront l'objet d'enquêtes plus approfondies: interrogatoires de leur entourage, parfois de leur employeur, mesures de surveillance rapprochée pouvant aller jusqu'aux écoutes téléphoniques. Résultat: zéro (aucune personne raisonnablement suspecte et encore moins condamnée pour terrorisme)¹⁰. On peut dire que l'inefficacité de cette méthode dans la lutte contre la criminalité est démontrée. Une méthode inefficace qui est pourtant loin d'être inoffensive. La Cour constitutionnelle allemande a fermement condamné le procédé, jugé stigmatisant pour toute une communauté religieuse et augmentant le risque de discrimination tant dans la vie quotidienne que sur le plan professionnel¹¹.

I. 2. Une interdiction du fichage politique toute relative

Au début des années 80, un scandale éblouissait la gendarmerie belge qui avait fiché consciencieusement des militants politiques et syndicaux sur les désormais célèbres « microfiches B »¹². En principe, la collecte des données qui révèlent les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'origine raciale ou ethnique, ou la vie sexuelle des personnes est strictement interdite¹³. Toutefois, la police dispose d'une dérogation à cette interdiction et peut donc récolter ce type de données sensibles. Selon quelles modalités? Cela reste assez flou¹⁴. En pratique, on constate néanmoins que le fichage

⁸ Comité P, rapport annuel 2001, p 40.

⁹ Comité P, rapport annuel 2001, p 42. www.comitep.be

¹⁰ Open Society Justice initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, p 68-69. Version originale en anglais: http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_20090526/profiling_20090526.pdf. Sommaire et recommandations en français: http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_20090526/french_20090609.pdf.

¹¹ Selon la Cour suprême allemande, la situation générale post 11 septembre ne peut pas justifier de telles atteintes à la vie privée. Seule des indices basés sur des faits concrets de préparation ou de commission d'actes terroristes pourraient le justifier. Décision du 4 avril 2006, citée par Open Society Justice initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, p 70, et par Olivier DE SCHUTTER et Julie RINGELHEIM, « Ethnic Profiling: A Rising Challenge for European Human Rights Law », *The Modern Law Review*, 2008, 71 (3), p 376.

¹² Voir à ce sujet: Colette BRAECKMAN, Marc DE KOCK, *Les libertés malades du pouvoir*, Bruxelles, Vie Ouvrière, 1980, p 231.

¹³ Art. 6 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après « LVP ») : « § 1er : Le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle, est interdit. » Le second paragraphe contient une série de dérogations à cette interdiction, notamment lorsqu'une loi permet le traitement des données sensibles, ou que la personne a donné son consentement.

¹⁴ L'art 44/1 al. 2 LFP prévoit qu'un arrêté royal doit fixer les modalités d'exercices. A l'heure où nous écrivons ces lignes (février 2010), cet AR n'a pas encore été adopté. L'option prise actuellement serait plutôt une modification législative (prévue avant l'été 2010).

politique a de beaux jours devant lui. En 2005, l'existence d'une liste intitulée « extremistische en terroristische groeperingen in Antwerpen »¹⁵) établie par la police d'Anvers a été rendue publique. Cette liste contenait de nombreuses associations ayant pignon sur rue, notamment pacifistes et interculturelles (Hand in hand, vaka, Forum voor vredesactie) et communautaires qualifiées de « ethnische groeperingen » (Unie van Turkse Verenigingen, Unie van moskeeën en islamistische verenigingen)¹⁶. Sous la rubrique « extreem links organisaties¹⁷ », on trouvait notamment les identités (parfois mal orthographiées) de quatre avocats, prétendument liés aux « advocaten voor het volk (Progressif (sic) Laywers Network) », ainsi que l'adresse de deux cabinets à Anvers. A ce jour, ils ne savent toujours pas pour quelles raisons précises ils étaient qualifiés d'« extrémistes » ou de « terroristes ».

I. 3. La Banque de données nationale générale (BNG) de la police intégrée

L'architecture policière belge actuelle¹⁸ est profondément marquée par le traumatisme de l'affaire Dutroux, marquée par la guerre des polices et la « rétention d'information » qui ont contribué au fiasco de l'enquête sur la disparition d'enfants¹⁹.

I. 3.1. Un « intérêt concret » en quête de définition précise

Désormais, toute information ayant un « intérêt concret » pour les missions judiciaires ou administratives de la police doit être stockée dans une banque de données nationale générale (BNG), une sorte de « référothèque centrale »²⁰ accessible à tous les policiers et magistrats du pays²¹. La notion d'« intérêt concret » n'est pas définie par la loi. Selon une directive de 2002, « le filtre essentiel est le fonctionnaire de police estimant que l'information dont il a pris connaissance est suffisamment importante que pour la reprendre »²². On peut se demander si un « filtre » qui repose sur le seul pouvoir d'appréciation du policier va effectivement jouer son rôle. La directive précitée fournit « quelques exemples d'informations constituant un intérêt concret pour l'exécution des missions de police », à savoir:

- « • la commission d'un hold-up dans un organisme bancaire (information concrète de police judiciaire);
- l'information donnée par un indicateur de plans visant à commettre un vol à main armée dans une pharmacie (information non concrète de police judiciaire);
- l'annonce de l'organisation d'une manifestation à Bruxelles durant un sommet européen (information concrète de police administrative);

¹⁵ Groupements extrémistes et terroristes à Anvers.

¹⁶ Le ministre de l'intérieur de l'époque a expliqué qu'il ne s'agissait que d'informations publiques ou fournies par les organisations elles-mêmes, ou d'information sur des « groupements à suivre » (Bull. Questions et réponses, Sénat, 2005-2006, n° 3-58, question n° 3-2874 de Mme Bousakla du 9 juin 2005. Le Comité P

¹⁷ Organisations d'extrême gauche

¹⁸ Celle-ci est régie essentiellement par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux (ci-après « LPI ») et, concernant certains aspects dont la BNG, par la loi du 5 août 1992 sur la fonction de police (ci-après « LFP »).

¹⁹ En 1995, la gendarmerie avait organisé une opération secrète de surveillance du pédophile Marc Dutroux, impliquant des moyens importants. Ce service n'a pas transmis des informations cruciales issues de cette « opération Othello » (comme l'existence de travaux d'aménagement dans les caves permettant la séquestration de personnes) aux enquêteurs et au juge d'instruction en charge de la disparition de deux fillettes alors séquestrées par M. Dutroux. Voir notamment Michel BOUFFIOLUX, Marie-Jeanne VAN HEESWYCK, La face cachée de l'enquête Dutroux et consorts, Charleroi, Couleur livres, 2004, pp. 37-83.

²⁰ Christophe CALIMAN, « La gestion de l'information policière dans la loi du 7 décembre 1998 et les principes relatifs à la protection de la vie privée », Revue de droit pénal et de criminologie, avril 2000, p 415.

²¹ Cette banque de données est gérée par le commissariat général de la police fédérale (art 44/4 LFP).

²² Directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative. (MB 18 juin 2002).

- l'information indiquant que des hooligans veulent perturber une rencontre de football en agressant les supporters de l'équipe adverse (information non concrète de police administrative)».

En principe, il doit s'agir d'informations objectives et vérifiées²³. Elles doivent aussi « présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent »²⁴. En pratique, ce garde-fou est peu opérant. Les « finalités » du travail policier recouvrent tant la recherche et la poursuite des infractions mais aussi tout l'aspect lié au maintien de l'ordre public (police administrative), qui peut s'interpréter de manière très large.

Le critère de « l'intérêt concret » est relativement flou et tranche avec la notion de « danger concret » défini comme « toute situation où il existe des présomptions suffisantes qu'une infraction pénale grave a été ou pourrait être commise à l'exclusion des possibilités éventuelles non assorties de preuves »²⁵

I. 3.2. A qui profite le doute?

Que faire en cas de doute sur l'intérêt concret? On aurait tendance à penser que le doute doit profiter aux personnes visées et qu'on ne procéderait pas à l'enregistrement des données douteuses. Pourtant, comme la rétention d'information est désormais passible de lourdes sanctions pour le policier²⁶, celui-ci aura tendance à procéder à la collecte des données en cas de doute. On peut donc se demander si l'absence d'enregistrement ne deviendra pas l'exception. Les exemples d'éléments non repris à la BNG sont rares dans la littérature²⁷: on cite les PV concernant les feux de cheminée, les différends familiaux ou le vandalisme dans des cabines téléphoniques publiques²⁸.

Comme on l'a vu plus haut, la directive actuellement appliquée par les policiers considère qu'une information « non concrète », c'est-à-dire, non vérifiée et non définitive, peut avoir un « l'intérêt concret ». Si le policier est le seul juge de « l'intérêt concret », rien n'empêche qu'une simple rumeur soit enregistrée dans la BNG.

²³ LFP 44/1 renvoie à la loi du 8 décembre 1992 sur la vie privée dont l'article 4 précise que : " Les données à caractère personnel doivent être :

1° traitées loyalement et licitement;

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, (...);

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour; toutes les mesures raisonnables doivent être prises pour que les données inexacts ou incomplètes, au regard des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;

5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. (...) ».

²⁴ Art 44/2 LFP.

²⁵ Recommandation R(87) 15, adoptée par le Comité des ministres du Conseil de l'Europe le 17 septembre 1987.) Christian de Valkeneer note que cette recommandation « a acquis un caractère quasi conventionnel puisqu'il y est fait référence dans la Convention d'application de l'Accord de Schengen (article 115), dans la Convention sur le Système d'information Douanier (article 8) et dans la Convention Europol (article 14) » (Ch. de VALKENEER, Manuel de l'enquête pénale, Larcier, 2006, p 345, note 729).

²⁶ Art. 41/11 LFP: « Tout fonctionnaire de police qui retient, sciemment et volontairement des informations et des données présentant un intérêt pour l'exécution de l'action publique ou le maintien de l'ordre public et s'abstient de les transmettre à la banque de données nationale générale, conformément à l'article 44/4, alinéa 3, sera puni d'un emprisonnement d'un mois à six mois et d'une amende de vingt-six à cinq cents francs, ou d'une de ces peines seulement. (...) ».

²⁷ L'art. 41/4 al. 4 LFP prévoit que les ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, déterminent, sur avis conforme de l'organe de contrôle visé à l'article 44/7, les catégories d'informations et de données qui n'exigent pas une transmission à la BNG. A notre connaissance, aucune liste publique de ces éléments n'existe à ce jour.

²⁸ G. BOURDOUX, A. LINERS, E. DE RAEDT, M. DE MESMAEKER, H. BERKMOES, La loi sur la fonction de police. Le Manuel de la fonction de police, Bruxelles, Politeia, 2005, p 300.

I. 3.3. Une inflation du nombre d'enregistrements dans la BNG

Tableau: Nombre d'entités enregistrées dans la BNG

Source : Rapport annuel du Comité P 2007-2008, p 36.

	2004	JUILLET 2006	DECEMBRE 2006	DECEMBRE 2007
FAITS CONCRETS	8 826 227	> 10 000 000	11 086 899	12 359 250
FAITS NON CONCRETS	INEXISTANT	COMPRIS DANS CHIFFRES CI-DESSUS	78 920	116 639
PERSONNES	1 425 904	1 764 052	1 644 435	1 745 208
VEHICULES	1 486 155	1 749 471	1 824 630	2 077 099
LIEUX	5 887	24 091	15 877	22 124
ENQUETES	INEXISTANT	PAS DE CHIFFRES	31 684	49 533
ORGANISATIONS	INEXISTANT	PAS DE CHIFFRES	11 547	18 886
NUMEROS	INEXISTANT	PAS DE CHIFFRES	72 923	108 507
OBJETS	11 641 688	14 590 426	15 390 444	17 464 197

On ne peut que s'inquiéter de l'inflation de ces chiffres. En forçant le trait, on peut affirmer que près d'un habitant sur six est répertorié dans la banque de données centralisée de la police intégrée. L'inflation du nombre de « faits non concrets » et des « organisations » est préoccupante lorsqu'on garde en mémoire les dérapages sur le fichage politique et sur l'absence de contrôle de la fiabilité des informations²⁹. De son côté, le comité P se réjouit de l'augmentation des données dans la BNG: parce que « il y a désormais moins de banques de données séparées et que de plus en plus de données sont centralisées (sic) dans une seule banque de données. Cela contribue à une meilleure coordination et accroît les possibilités de contrôle, mais cela offre également la possibilité de corriger des données (gestion uniforme, application de règles de ventilation, plaintes vie privée, etc.) »³⁰. Quelques paragraphes plus loin dans son rapport, le Comité P se contredit et constate également qu'il existe, à côté de la BNG de très nombreuses autres banques de données de toute sorte (drogues, prostitution, délinquance juvénile, albums photos, assignations à résidence, cyclomoteurs, etc.) dont « personne n'a d'idée exacte de leur nombre ni, *a fortiori*, de leur contenu. »³¹. Selon la Commission pour la protection de la vie privée (ci-après « CPVP »), les services de

²⁹ Sur ce dernier point, voir plus loin.

³⁰ Comité P, rapport annuel 2007-2008, www.comitep.be

³¹ Ibid.

polices ont déclaré 633 traitements de données entre 1995 et 2001. Entre 2001 et 2005, ce chiffre n'est que de 89³². Alors que le grand nombre de ces fichiers inquiète³³, il est pour le moins ardu, pour le citoyen, de prendre connaissance de la liste exhaustive³⁴.

I. 3.4. Temps de conservation? Indéterminé!

Ce constat est renforcé par l'absence de délai de conservation prévu par un texte. Les déclarations effectuées à la CPVP mentionnent une durée prévue de conservation de 5 ans pour les missions de police administrative et de 10 ans pour les missions judiciaires (voir annexes). Ces mentions sont indicatives. Actuellement, les données de la BNG sont donc conservées pour une durée indéterminée, en attendant qu'une loi vienne clarifier les choses³⁵. Il n'y a aucune règle claire concernant la suppression ou l'effacement des données.

I. 3.5. Transmission des informations à d'autres autorités belges et étrangères

Les policiers peuvent transmettre des informations figurant dans leurs banques de données aux autorités judiciaires, aux services de polices (belges ou étrangers), aux services de renseignements et de sécurité, au comité P, au comité R, à l'OCAM³⁶, à l'inspection générale de la police fédérale et de la police locale, et aux organisations internationales de coopération policière à l'égard desquelles les autorités belges ont des obligations (notamment Interpol et Europol). Le service de police qui transmet les données doit vérifier si le destinataire en a besoin pour exécuter ses missions légales et si cette transmission est indispensable³⁷.

Par ailleurs, les policiers doivent informer les autorités administratives (bourgmestre ...) des « événements extraordinaires concernant l'ordre public », « des faits importants qui sont de nature à troubler la tranquillité, la sécurité ou la salubrité publique » dans la commune³⁸. Ils doivent aussi informer les autorités militaires « de tout ce qui peut porter atteinte à la sûreté des forces armées » et « de toute propagande incitant les militaires à l'indiscipline »³⁹.

I. 4. Signalement: « petites » erreurs, graves conséquences

Dans les années 90, une ressortissante belge a dû attendre pendant trois ans la délivrance d'un visa parce qu'elle était signalée à tort au Bulletin Central de Signalements (BCS) à la suite d'une transcription erronée d'une demande émanant d'Interpol Washington et d'une correction incomplète de la mention fautive (il s'agissait d'un homonyme encodé avec une date de naissance erronée, celle de la victime)⁴⁰. Au cours de

³² Chiffres récoltés par Liesbeth DE VIEGER, Nathalie VERSTUYFT, « Politiregisters en privacy », Gert VERMEULEN (ed.), Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen, Anvers / Appeldoorn, Maklu, 2007, p. 233.

³³ Dans son avis n° 13/98 du 23 mars 1998 portant sur l'avant-projet de réorganisation des services de police, la Commission de la protection de la vie privée a dénoncé les risques qui découlent de la prolifération des traitements de données et des flux d'informations.

³⁴ Un répertoire central est tenu par l'organe de contrôle ad hoc mais n'est accessible qu'« au Ministre de l'Intérieur ou à son délégué, au Ministre de la Justice ou à son délégué, aux autorités de contrôle compétentes, aux autorités judiciaires, aux autorités de police administrative et aux services de police ». (art 6 de l'AR du 30 mai 2002 déterminant les conditions d'exercice des missions de l'organe de contrôle visé à l'article 44/7 de la loi sur la fonction de police, M.B. 14 juin 2002). Sur le registre public de la CPVP, voir plus loin.

³⁵ Un projet d'arrêté royal a été rédigé par le ministre de la justice en 2008 mais a fait l'objet de critiques qui ont abouti à impliquer le parlement dans ce débat. Un groupe de travail (le « groupe 44 ») est actuellement en train de discuter de ces questions. La presse évoque un projet de loi pour l'été 2010.

³⁶ L'Organe de coordination pour l'analyse de la menace, créé par la loi du 10 juillet 2006.

³⁷ G. BOURDOUX, A. LINERS, E. DE RAEDT, M. DE MESMAEKER, H. BERKMOES, op. cit., 2005, p 295.

³⁸ Art. 5/2 LFP.

³⁹ Art. 5/4 LFP.

⁴⁰ Rapport extraordinaire 1999 du comité P, point 6.1.1.

la même période, un officier de réserve signalé au B.C.S., à la demande des autorités militaires pour des raisons essentiellement administratives, est tiré du lit à 5 h 30 du matin lors d'un contrôle des fiches de l'hôtel où il séjourne, et ensuite emmené au poste de police et incarcéré sans que personne ne se soucie des véritables raisons de signalement au B.C.S.⁴¹.

Ces exemples démontrent, si besoin était, que le respect du droit à la vie privée et du traitement correct des données personnelles n'est pas qu'une affaire théorique ou abstraite. Une simple négligence commise soit lors de l'encodage, soit lors de la lecture des données d'un signalement peuvent avoir des conséquences qui dépassent de loin la vie privée pour aboutir à des violations d'autres droits fondamentaux bien plus palpables (en l'occurrence ici la liberté de circuler et la liberté tout court).

Selon le Comité P « il s'impose d'avertir, de manière très explicite, les fonctionnaires chargés des affaires ayant trait aux droits fondamentaux des citoyens de leur responsabilité individuelle, ainsi que de la nécessité de travailler d'une manière rigoureuse. ». Il estime aussi qu'il est « impératif de pouvoir identifier avec précision, à chaque stade de la procédure, le fonctionnaire traitant, ainsi que le responsable de la gestion afin de déterminer la responsabilité individuelle, ou organisationnelle, ou structurelle en cas de manquement »⁴².

I. 5. La « tricoche » ou consultation abusive des fichiers : anecdotique?

Aux menaces de violation de la vie privée induites par les pratiques décrites plus haut, vient s'ajouter un vieux phénomène : les consultations abusives de fichiers par des policiers qui « oublient » que leurs pouvoirs ne peuvent s'exercer qu'au service exclusif de l'intérêt général et de leurs missions légales⁴³. La pratique peut être motivée par la simple curiosité (regarder si une célébrité est « connue des services »⁴⁴, pour « rendre service » à un ancien collègue recyclé dans le privé ou à un journaliste. Lorsque le policier obtient une contrepartie, on parle de « tricoche » dans le jargon policier français⁴⁵. Il est difficile de connaître avec précision l'ampleur du problème mais, même s'il était limité, le fait que des données sensibles puissent être transmises à des personnes non autorisées est très préoccupant. D'autant plus que, comme on l'a vu, chaque policier peut accéder à la BNG. Une traçabilité précise des consultations s'impose. Le Comité P plaide pour que l'on « intervienne sévèrement » à l'égard des policiers qui consultent des données personnelles en dehors du cadre de leurs missions de police judiciaire et administrative⁴⁶. Sera-t-il entendu?

Cet échantillon de certaines pratiques policières nous semble illustrer à suffisance le besoin d'un contrôle démocratique du fichage policier. Tentons à présent de décrire brièvement comment s'opère celui-ci au regard des dispositions légales en vigueur actuellement en Belgique.

⁴¹ Ibid.

⁴² Rapport extraordinaire 1999 du comité P, point 6.1.2.

⁴³ Ce principe fondamental est posé par l'article 12 de la Déclaration des droits de l'homme et du citoyen en 1789, cité en exergue de la présente contribution.

⁴⁴ Au lendemain du suicide de la chanteuse flamande Yasmine en septembre 2009, plus de 900 policiers ont consulté ses données personnelles De Morgen, 18/09/2009 <http://www.demorgen.be/dm/nl/989/Binnenland/article/detail/997727/2009/09/18/918-politiemensen-snuffelen-in-gegevens-Yasmine.dhtml>

⁴⁵ Assemblée nationale, Rapport d'information cité, pp. 143-149.

⁴⁶ Comité P, rapport annuel 2007-2008, p 40.

II. Quel droit de regard du citoyen sur les fichiers policiers en Belgique?

II. 1. Les principes de base sur la protection de la vie privée et des données personnelles

Avant d'entamer l'examen des fichiers policiers, il est nécessaire de rappeler sommairement quelques principes de base qui s'appliquent aux fichiers de données personnelles en général. Ceci permettra de mieux comprendre la portée des dérogations dont bénéficie la police.

La loi du 8 décembre 1992 sur la protection de la vie privée à l'égard des traitements de données à caractère personnel⁴⁷ a apporté un cadre précis à matière et a mis en place la Commission pour la protection de la vie privée, un organe formellement rattaché à la Chambre des représentants⁴⁸, compétent notamment pour donner des avis et recommandations et pour contrôler le respect de la loi.

II. 1.1. Les droits de la personne fichée vis-à-vis du responsable du traitement

Les garanties fondamentales qui offrent au citoyen une protection contre les abus peuvent être résumées comme suit:

- 1) déclaration obligatoire à la CPVP pour tout fichier automatisé qui figure dans le registre public⁴⁹
- 2) obligation du « responsable du traitement » de fournir, dès le début de la récolte, certaines informations aux personnes dont il traite les données, notamment: la finalité du traitement, le nom et l'adresse du responsable du traitement, la possibilité de s'opposer au marketing direct, l'existence d'un droit d'accès⁵⁰
- 3) droit inconditionnel, pour tout personne prouvant son identité, d'obtenir de la part du responsable du traitement, au plus tard 45 jours après sa demande datée et signée:
 - a) la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées;
 - b) la communication, sous une forme intelligible, des données faisant l'objet des traitements, ainsi que de toute information disponible sur l'origine de ces données;
 - c) la connaissance de la logique qui sous-tend tout traitement automatisé des données la concernant, dans le cas de décisions automatisées;
 - d) un avertissement de la faculté d'exercer les recours prévus aux articles 12 et 14 et, éventuellement, de consulter le registre public de la CPVP⁵¹.

⁴⁷ Version consolidée disponible sur: http://www.privacycommission.be/fr/static/pdf/wetgeving/loi_vie_privée.pdf Voir aussi le document explicatif de la CPVP intitulé La protection des données à caractère personnel en Belgique, 8 février 2007, 28 p.: http://www.privacycommission.be/fr/static/pdf/cbpl-documents/note_vie-priv-e-g-n-ralit-s.pdf

Voir aussi la version de la loi annotée contenant de très nombreuses références de jurisprudence recueillies par la CPVP, qui met à la disposition du public un instrument de travail incontournable sur le sujet: <http://www.privacycommission.be/fr/static/pdf/wetgeving/codex-fr-31-01-08-website-doc.pdf>

⁴⁸ La CPVP est composée de 8 membres effectifs et 8 membres suppléants, nommés pour 6 ans par la Chambre sur proposition du gouvernement, et présidée par un magistrat (art. 23 et suivants LVP).

⁴⁹ Ceci signifie que les fichiers « papier » ne doivent pas être déclarés. Cependant, l'art. 19 LVP stipule que : « Lorsque la Commission de la protection de la vie privée estime qu'un traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier est susceptible de porter atteinte à la vie privée, elle peut soit d'office, soit sur requête d'une personne concernée enjoindre au responsable du traitement de lui communiquer tout ou partie des informations énumérées à l'article 17 ».

⁵⁰ Art. 9 LVP.

⁵¹ Art. 10 § 1er LVP.

4) droit, sur simple demande datée et signée adressée au responsable du traitement:

- a) d'obtenir sans frais la rectification de toute donnée inexacte⁵²;
- b) de s'opposer, « pour des raisons sérieuses et légitimes tenant à une situation particulière »⁵³, à ce que des données personnelles fassent l'objet d'un traitement⁵⁴;
- c) d'obtenir sans frais la suppression ou l'interdiction d'utilisation de toute donnée personnelle incomplète ou non pertinente pour le but du traitement, ou dont l'enregistrement, la communication ou la conservation sont interdits ou encore qui a été conservée au-delà de la période autorisée.

5) obligation, pour le responsable du traitement, de communiquer, dans le mois de la demande, les rectifications ou effacements des données effectués, ou la suite donnée à une demande d'opposition, à la personne concernée ainsi qu'aux personnes à qui les données incorrectes, incomplètes et non pertinentes ont été communiquées « pour autant qu'il ait encore connaissance des destinataires de la communication et que la notification à ces destinataires ne paraisse pas impossible ou n'implique pas des efforts disproportionnés »⁵⁵.

II. 1.2. Recours judiciaire spécifique et dédommagement par le responsable du fichier

La personne dont les droits décrits ci-dessus n'ont pas été respectés peut introduire un recours auprès du président du tribunal de première instance, selon une procédure urgente⁵⁶. Ce recours n'est recevable que si une demande d'accès ou de rectification a été rejetée ou s'il n'y a pas été donné suite dans le délai⁵⁷. En cas de « motifs impérieux » de craindre que le responsable du fichier dissimule ou fasse disparaître les données personnelles litigieuses, on peut saisir le juge par requête unilatérale pour qu'il ordonne toute mesure de nature à éviter cette dissimulation ou cette disparition. Pendant toute la procédure, le responsable du traitement doit indiquer clairement, lors de toute communication d'une donnée litigieuse, que celle-ci est contestée⁵⁸.

Si une personne subit « un dommage causé par un acte contraire aux dispositions déterminées par ou en vertu de la présente loi », c'est le responsable du traitement qui doit dédommager la personne lésée, sauf s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable⁵⁹.

II. 1.3. Certaines garanties inapplicables aux fichiers policiers

Les autorités publiques qui traitent des fichiers à des fins de police judiciaires, les services de police et les autres autorités qui traitent des données pour des missions de police administrative⁶⁰, sont dispensées des

⁵² Art. 12 §1er, al. 1 LVP.

⁵³ Art 12 §1er, al. 2 LVP.

⁵⁴ Cette faculté n'existe pas pour les traitements nécessaires soit l'exécution d'un contrat (ou de mesures précontractuelles) auquel la personne concernée est partie, soit au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance (art. 12 §1er al 2 renvoyant à l'art. 5 b) et c) LVP).

⁵⁵ Art. 12 § 3 LVP.

⁵⁶ « comme en référé », selon l'art. 14 LVP.

⁵⁷ Art. 14 §5 LVP.

⁵⁸ Art. 15 LVP.

⁵⁹ Art. 15 bis LVP.

⁶⁰ Art. 3 §5 LVP. Pour le traitement à des fins de police administrative, tous les services de police visés à l'article 3 de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements sont dispensés. Les autres autorités doivent avoir été désignées par arrêté royal délibéré en Conseil des ministres, après avis de la CPVP pour pouvoir bénéficier de la dispense.

obligations décrites ci-dessus, à l'exception de l'obligation de déclaration⁶¹. Cela signifie que le citoyen n'a pas le droit d'être averti que ses données personnelles sont utilisées par la police. Il n'a pas non plus le droit d'obtenir des informations sur les fichiers auprès du responsable du traitement, et encore moins solliciter la rectification ou la suppression de données. Notons cependant que, pour le surplus, la constitution et la gestion de fichiers policiers doit s'effectuer conformément à toutes les dispositions de la loi sur la protection de la vie privée auxquelles il n'a pas été dérogé⁶².

II. 2. Le droit de connaître l'existence d'un fichier policier

Il est théoriquement possible de connaître l'existence de tous les fichiers automatisés⁶³ de données personnelles gérés par la police. En effet, celle-ci est tenue d'effectuer une déclaration auprès de la Commission pour la protection de la vie privée pour tout « mise en œuvre d'un traitement entièrement ou partiellement automatisé »⁶⁴. La déclaration doit mentionner obligatoirement un certain nombre d'éléments dont le nom du fichier, sa finalité, les coordonnées complètes du « responsable du traitement, la durée de conservation des données, les garanties qui entourent une éventuelle transmission à des tiers. » Il n'est pas inutile de remarquer que l'absence de déclaration est sanctionnée pénalement⁶⁵. On retrouve donc un certain nombre de fichiers policiers dans le registre public de la CPVP, accessible à l'adresse:

<https://www.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=fr>

Pourtant, en pratique, la chasse aux informations n'est pas des plus aisées parce que les méthodes de déclaration ne sont pas uniformes et que les fonctionnaires qui remplissent la déclaration sont souvent assez avares de renseignements précis. Tenter de dresser un inventaire exhaustif des fichiers policiers relève de la gageure, d'autant plus que le Comité P suspecte certaines grandes zones de police d'exploiter des fichiers sans avoir effectué de déclaration à la CPVP⁶⁶. Notons enfin que pour les services de renseignements, ce problème ne se pose pas: ils échappent totalement à cette obligation de déclaration⁶⁷.

II.3. Pas de droit de savoir si on figure ou non dans un fichier policier

II. 3.1. L'accès indirect via la Commission pour la protection de la vie privée (CPVP)

En Belgique, l'accès direct aux données dont dispose la police n'est pas permis. Il faut obligatoirement passer par l'intermédiaire de la CPVP, qui peut opérer ce contrôle, à la demande de la personne visée⁶⁸. Pour ce faire, il faut envoyer une demande datée et signée à la Commission. Sous peine d'irrecevabilité, la demande doit contenir: nom, prénom, date de naissance, nationalité de la personne concernée, une photocopie de son document d'identité. Il faut aussi désigner l'autorité ou le service concerné et « tous les éléments pertinents

⁶¹ En vertu de l'art. 3 §5 LVP, les articles 9, 10, § 1er, et 12 ne s'appliquent pas.

⁶² L'art. 44/2 LFP soumet la collecte, le traitement et la transmission des informations et des données policières au respect de la LVP et précise que « ces informations et données doivent présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent ».

⁶³ Comme on l'a vu, un particulier qui estime qu'un fichier non automatisé porte atteinte à sa vie privée peut demander à la CPVP qu'elle ordonne au service de police d'effectuer une déclaration concernant ce fichier (art. 19 LVP).

⁶⁴ art. 17 LVP.

⁶⁵ D'une amende de cent euros à cent mille euros (art. 39, 7° LVP).

⁶⁶ Comité P, rapport annuel 2007-2008, www.comitep.be

⁶⁷ Art. 3 § 4 LVP.

⁶⁸ La procédure est prévue par l'article 13 de la loi du 8 décembre 1992 et les articles 36 et suivants de l'AR du 13 février 2001 portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (MB 13 mars 2001).

concernant les données contestées, tels que leur nature, les circonstances ou l'origine de la prise de connaissance des données contestées, ainsi que les rectifications éventuellement souhaitées.⁶⁹»

La CPVP peut exiger que la police rectifie ou efface des données erronées concernant une personne⁷⁰. Mais elle n'a en principe pas le droit d'informer le plaignant de ce qui a été fait concrètement. Le plaignant n'aura, le plus souvent, pas d'autre information qu'un avis lui signalant que « les vérifications nécessaires ont été effectuées »⁷¹. La personne ne peut donc pas savoir si elle figurait ou non dans le fichier, et encore moins quelles données s'y trouvaient. Il lui est tout aussi impossible de savoir si des données ont été corrigées ou effacées. Il faut attendre un an avant de réintroduire une demande concernant les mêmes données, sauf dérogation de la CPVP accordée sur demande motivée⁷².

Compte tenu de ces limites, il n'est pas étonnant que cette procédure soit si peu utilisée. En 2008, la Commission a été saisie 159 fois⁷³. Ce chiffre représente une forte augmentation par rapport à 2007⁷⁴. Cette procédure est-elle pour autant totalement inutile? Pas du tout, s'il faut croire la CPVP, qui mentionne que près de trois quart des demandes clôturées en 2008 ont donné suite à une suppression totale ou partielle des données, comme le montre le tableaux ci-dessous.

Analyse des « dossiers 13 » clôturés en 2008 (13-2007 et 13-2008)

	Nombre	%
Suite donnée		
Suppression complète	33	56,90
Suppression partielle	10	17,24
Conservation des données	10	17,24
Pas enregistré	5	8,62
délai moyen de réponse (jours calendrier)	132,48	

Source : Rapport CPVP 2008, p 70.

Malgré les limites de cette procédure, nous ne pouvons qu'encourager les personnes qui souhaiteraient contester un fichage potentiel d'user de leurs droits. Un modèle de demande, extrait du site internet de la CPVP, figure en annexe de la présente contribution. Selon certains, la dérogation aux droit d'accès et de rectification qui existe actuellement en Belgique au sujet des fichiers policiers est trop large et mériterait une modification de la loi⁷⁵.

⁶⁹ Article 37 de l'AR du 13 février 2001 précité.

⁷⁰ A l'encontre d'un service de police, la Commission « effectue ou ordonne toute vérification qu'elle estime utile », et « peut faire rectifier ou effacer des données, ainsi que insérer des données divergentes par rapport aux données traitées par le service concerné. Elle peut interdire la communication des données. » (Article 43 de l'AR du 13 février 2001 précité). Notons qu'à l'encontre des services de renseignements, la Commission ne peut que recommander « les mesures qu'elle estime nécessaire », sans aucun pouvoir de contrainte.

⁷¹ Article 46 de l'AR du 13 février 2001, précité. La Commission peut, après avoir pris l'avis des policiers, donner toute autre information qu'elle estime appropriée mais uniquement pour les données servant au contrôle d'identité.

⁷² Art 40 de l'AR du 13 février 2001 précité.

⁷³ Rapport annuel 2008 de la CPVP, p 56.

⁷⁴ En 2007: 87 demandes; en 2006: 91 demandes (CPVP, Rapport annuel 2007, p 60.)

⁷⁵ Liesbeth DE VIEGER, Nathalie VERSTUYFT, « Politierregisters en privacy », Gert VERMEULEN (ed.), Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen, Anvers / Appeldoorn, Maklu, 2007, p. 227.

II. 3.2. L'organe de contrôle ad hoc de la police intégrée⁷⁶

La loi du 7 décembre 1998 sur la police intégrée a mis en place un organe de contrôle interne à la police, chargé spécifiquement de la BNG et de la bonne application des pratiques policières en matière d'information⁷⁷. Il est donc en pratique un interlocuteur fréquent de la CPVP lorsqu'elle opère des contrôles. Cet organe est composé d'un membre de la police locale, d'un membre de la police fédérale et d'un expert. Il est présidé par un magistrat fédéral désigné par le ministre de la Justice et le ministre de l'Intérieur sur proposition du procureur fédéral, mais qui agit, pendant la durée de sa désignation, « de manière indépendante à l'égard du parquet fédéral »⁷⁸. Cet organe « n'a d'autre contrôle, sur les services de police et les membres de la police, que celui qui porte sur la manière dont ils participent au concept global de gestion de l'information : n'ont-ils pas retenu de l'information. A-t-on créé des banques de données particulières sans autorisation. A-t-on pris connaissance de données dont on avait (sic) pas besoin pour l'exercice de la fonction ("need to know"), etc. »⁷⁹. Son utilité pour le citoyen est quasi-nulle parce qu'aucun texte ne prévoit qu'on puisse s'adresser à lui⁸⁰. Aucun texte ne l'interdit formellement non plus, donc pourquoi ne pas tenter d'obtenir une correction en lui soumettant des éléments? Reste à voir si les oreilles de l'organe de contrôle seront attentives aux doléances fondées sur le droit à la vie privée. Il ressort du dernier rapport annuel du Comité P que l'organe de contrôle travaille surtout à une meilleure récolte des données, regrettant que les empreintes digitales, les photos et les descriptions physiques complètes de personnes arrêtées ne figurent pas systématiquement dans la BNG⁸¹. Les missions de cet organe se chevauchent en partie avec celles, plus larges, de la Commission pour la protection de la vie privée et du comité P. L'argument du risque de cumul de compétences avec le comité P et la CPVP avait été brandi par le gouvernement en 2002 pour justifier la limitation des pouvoirs de l'organe de contrôle. Selon le Conseil d'Etat, cette limitation est illégale : « Si la loi a jugé utile de multiplier les contrôles, il n'appartient pas au Roi de limiter ceux-ci pour éviter les chevauchements »⁸².

Comme nous l'avons vu, le citoyen ne dispose pas d'un véritable droit de regard sur ses données personnelles recueillies par les services de police. Il doit se contenter d'un droit d'accès indirect et est prié de placer une confiance aveugle dans la Commission pour la protection de la vie privée. Même si celle-ci possède un véritable pouvoir d'injonction pour ordonner à la police d'effacer des données, on peut se demander si ce mécanisme respecte les droits fondamentaux.

⁷⁶ Voir art. 44/7 LFP et l'arrêté royal du 30 mai 2002 déterminant les conditions d'exercice des missions de l'organe de contrôle visé à l'article 44/7 de la loi sur la fonction de police (MB 14 juin 2002).

⁷⁷ Il s'agit d'évaluer leur conformité aux articles 44/1 à 44/9 de la LFP (insérés par la LPI).

⁷⁸ Art. 44/7 al. 5 LFP.

⁷⁹ Extrait du rapport au Roi précédant l'AR du 30 mai 2002 précité.

⁸⁰ Voir l'arrêté royal du 30 mai 2002 précité. Voir aussi le règlement d'ordre intérieur du 17 juin 2003 (M.B. 9 septembre 2003).

⁸¹ « Ils ont contrôlé, sur la base de listes de personnes arrêtées (cf. registre des personnes arrêtées), pour qui la « triple identification » judiciaire (photos, empreintes digitales et description individuelle) avait été effectuée correctement. Lors d'un contrôle des données transmises à la BNG en la matière pour 12 383 personnes, il est apparu que (1) aucune photo n'était présente dans 68 % des cas, (2) la description individuelle manquait pour 73 % des personnes et (3) il n'y avait pas d'empreintes digitales dans 60 % des cas. » Ceci recèlerait « un très grave danger » qui empêcherait d'identifier des auteurs éventuels. Comité P, rapport annuel 2007-2008, p 38. www.comitep.be

⁸² Avis du Conseil d'Etat N° 31.932/2 annexé à l'AR du 30 mai 2002 (M.B. 14 juin 2002). Sur le contrôle exercé par le comité P, voir la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements.

III. Conformité de la pratique belge avec la Convention européenne des droits de l'homme

Il paraît intéressant de confronter le mécanisme de contrôle décrit plus haut avec quelques décisions importantes de la Cour européenne des droits de l'homme sur des questions de droit à la vie privée, et de recours effectif.

III. 1. Le droit à la vie privée (article 8)

L'article 8 de la Convention européenne des droits de l'homme est rédigé comme suit:

- «1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

III. 1.1. Définition de la vie privée dans le cadre du fichage

Certains États ont défendu la thèse selon laquelle les activités publiques (réunions ouvertes, manifestations, pétition sur internet, publication de brochures politiques...) pouvaient faire l'objet d'un contrôle et d'un fichage sans limite parce qu'elles ne relèveraient pas de la sphère privée protégée par cette disposition. La Cour a fermement rejeté cette interprétation restrictive. Se référant à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, elle considère que « toute information concernant une personne physique identifiée ou identifiable » faisant l'objet d'un traitement automatisé peut porter atteinte à la vie privée⁸³. Elle affirme aussi que « des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics » et que « Cela vaut davantage encore lorsque ces données concernent le passé lointain d'une personne »⁸⁴.

III. 1.2. Existence d'une ingérence

Selon la Cour, « tant la mémorisation par une autorité publique de données relatives à la vie privée d'un individu que leur utilisation et le refus d'accorder la faculté de les réfuter constituent une ingérence dans le droit au respect de sa vie privée garanti par l'article 8 § 1 de la Convention »⁸⁵. On peut se demander si le système belge ne s'apparente pas à un « refus d'accorder la faculté de réfuter » des données puisqu'on ne peut pas s'adresser directement à la police pour contester les données. En outre, lorsqu'on s'adresse à la CPVP, on ne peut jamais savoir si des données ont été corrigées ou non, sauf s'il s'agit d'une faute

⁸³ Cour EDH, *Amann c. Suisse* [GC], du 16 février 2000, disponible, comme tous les arrêts cités, sur <http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-fr>

⁸⁴ Cour EDH, *Rotaru c. Roumanie*, du 4 mai 2000, § 43. voir toutefois l'opinion dissidente du juge Bonello pour qui « Le militantisme public au sein de partis politiques publics n'a (...) rien à voir avec le principe qui commande d'élever la protection de la vie privée au rang de droit fondamental. » (§ 6). La Cour a confirmé sa jurisprudence dans l'affaire *Segerstedt-Wiberg et autres c. Suède* du 6 juin 2006, § 72.

⁸⁵ arrêts *Leander* précité, p. 22, § 48, *Kopp c. Suisse* du 25 mars 1998, Recueil 1998-II, p. 540, § 53, et *Amann* précité, §§ 69 et 80, *Rotaru* précité, § 46.).

d'identité. Pour la Cour, le refus d'informer les personnes de l'intégralité des renseignements à leur sujet qui sont conservés dans le fichier secret de la police s'analyse en une ingérence dans l'exercice de leur droit au respect de leur vie privée⁸⁶. Il n'y a donc peu de doute sur le fait que le fichage policier, tel qu'il est par exemple centralisé au niveau de la BNG, constitue une ingérence au sens de l'article 8. Cette ingérence est acceptable uniquement si elle est prévue par la loi, si elle poursuit un but légitime visé au second paragraphe, et enfin, si elle est nécessaire dans une société démocratique. Examinons brièvement chacun de ces éléments.

III. 1.3. Ingérence prévue par la loi

Pour la Cour de Strasbourg, les mots « prévue par la loi » imposent non seulement que la mesure incriminée ait une base en droit interne, mais visent aussi la qualité de la loi en cause : ainsi, celle-ci doit être accessible au justiciable et prévisible⁸⁷. Une norme est « prévisible » lorsqu'elle est rédigée avec assez de précision pour permettre à toute personne, en s'entourant au besoin de conseils éclairés, de régler sa conduite. Ceci implique que la loi doit offrir une certaine protection contre des atteintes arbitraires de la puissance publique au droit à la vie privée. Elle souligne que le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret. Il convient par conséquent de définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire.⁸⁸

En Belgique, c'est le concept d'« intérêt concret » qui est le sésame qui ouvre grand les portes de la BNG permettant à quantités d'informations de s'y engouffrer. Il est permis de douter qu'il remplisse la condition de « netteté suffisante », d'autant plus qu'il permet, à l'heure actuelle, une conservation illimitée des données, puisque l'arrêté royal censé réglementer les modalités du traitement de l'information policière se fait attendre depuis plus de 12 ans. Dans l'affaire Rotaru précitée, c'est notamment l'absence de durée de conservation fixée par la loi qui a amené la Cour à considérer que l'ingérence n'était pas « prévue par la loi »⁸⁹.

On note également que les données sensibles liées notamment à l'origine ethnique, aux opinions politiques, aux affiliations syndicales sont aujourd'hui allègrement récoltées et traitées. Ceci ressort très clairement de certaines déclarations concernant des fichiers policiers présentes dans le registre public de la CPVP. A titre d'exemple, dans la rubrique « données pouvant être fournies » concernant la partie administrative de la BNG, on trouve non seulement les données d'identification traditionnelles (nom, adresse, tél., ...), électronique (adresses IP, cookies, ...) et « biométriques », mais aussi « profession et emploi », les « affiliations » sans autre précision (mutualiste, syndicale?), les « données raciales ou ethniques », les « opinions politiques », et les « convictions religieuses ou philosophiques » (voir annexe). Or, si la loi autorise bel et bien la police à traiter des données sensibles, ce traitement doit s'effectuer « selon les modalités déterminées par le Roi, après avis de la Commission de la protection de la vie privée »⁹⁰. Or, comme on le sait, depuis la loi de 1998 créant la BNG, aucun arrêté royal n'a été adopté pour fixer lesdites modalités de traitement. Ceci pose un véritable problème si l'on tient compte, comme le fait constamment la Cour européenne des droits de l'homme, de l'importance des « garanties adéquates et suffisantes contre les abus, car un système de

⁸⁶ Cour ECH Segerstedt-Wiberg et autres c. Suède du 6 juin 2006, § 99.

⁸⁷ Voir notamment l'arrêt Amann précité, § 50.

⁸⁸ Cour EDH, Malone c. Royaume-Uni du 2 août 1984, § 67, repris dans l'arrêt Amann précité, § 56 et Rotaru précité, § 55).

⁸⁹ Affaire Rotaru, précitée, § 57.

⁹⁰ Art 41/1 al. 2 LFP.

surveillance secrète destiné à protéger la sécurité nationale comporte le risque de saper, voire de détruire, la démocratie au motif de la défendre »⁹¹.

III. 1.4. Poursuite d'un but légitime

Il y a peu de doutes sur le fait que la constitution de fichiers policiers remplit un objectif légitime visé au § 2 de l'article 8⁹².

Dans une intéressante affaire jugée le 6 juin 2006, la Cour de Strasbourg a considéré que la conservation, par les services de renseignement suédois, d'informations relatives à la participation d'une personne à une réunion politique à Varsovie en 1967, « compte tenu de la nature de ces renseignements et de leur ancienneté (...) ne se fondait pas sur des motifs pertinents et suffisants au regard de la protection de la sécurité nationale »⁹³. La Cour ajoute: « De même, la conservation de la majeure partie des informations divulguées au cinquième requérant ne peut guère passer pour répondre à des intérêts de sécurité nationale véritablement pertinents pour l'Etat défendeur. La conservation des renseignements selon lesquels l'intéressé aurait, en 1969, préconisé d'opposer une résistance violente aux contrôles de police durant des manifestations se fonde sur des motifs qui, malgré leur caractère pertinent, ne sauraient passer pour suffisants trente ans plus tard »⁹⁴. On pourrait déduire de ceci que le but cesse d'être légitime si la conservation des données n'a plus de lien raisonnablement justifié avec ce but.

Thomas Hammarberg, commissaire aux droits de l'homme du Conseil de l'Europe, définit de la manière suivante les exigences à remplir pour répondre au principe de finalité:

- « • il importe d'être aussi précis que possible; il ne suffit pas d'indiquer que le traitement de données envisagé entre dans le cadre du travail de police ni même d'une tâche spécifique (enquête et poursuites pénales, réaction à une menace immédiate ou encore – plus discutablement – prévention) ;
- les données à caractère personnel collectées pour un besoin de police particulier (parer une menace, par exemple) ne peuvent être utilisées à d'autres fins (enquêter sur une infraction, par exemple) que si elles auraient pu être recueillies dans ce second but de manière indépendante ;
- les données à caractère personnel ne doivent jamais être collectées par la police ou d'autres services chargés de l'application de la loi « au cas où »⁹⁵.

Une fois encore, on peut se demander si le caractère peu précis de l' « intérêt concret » pour l'ensemble des missions de police remplit cette exigence de finalité.

⁹¹ Cour EDH, arrêt Klass et autres c. Allemagne du 6 septembre 1978, 23-24, §§ 49-50.

⁹² Relevons toutefois l'opinion concordante de M. Wildhaber, à laquelle M. Makarczyk, M. Türmen, M. Costa, Mme Tulkens, M. Casadevall et Mme Weber déclarent se rallier, suite à l'arrêt Rotaru précité: « Quant à la question du but légitime, la Cour admet d'ordinaire sans difficulté la légitimité de l'objectif défini par le Gouvernement sous réserve qu'il relève de l'une des catégories visées au paragraphe 2 des articles 8 à 11. Toutefois, pour la sécurité nationale comme pour d'autres buts, j'estime qu'il doit exister au moins un lien raisonnable et réel entre les mesures portant atteinte à la vie privée et l'objectif invoqué pour que celui-ci puisse être considéré comme légitime. A mon sens, expliquer que la conservation, pour ainsi dire sans discernement, d'informations relatives à la vie privée d'individus correspond à un souci légitime de sécurité nationale pose manifestement un problème. ».

⁹³ Cour EDH, Segerstedt-Wiberg et autres c. Suède, 6 juin 2006, § 90.

⁹⁴ Ibid.

⁹⁵ Commissaire aux droits de l'homme du Conseil de l'Europe, Lutte contre le terrorisme et protection du droit au respect de la vie privée, CommDH/IssuePaper(2008)3, p. 9.

III. 1.5 . Nécessaire dans une société démocratique

Pour qu'une ingérence soit acceptable en application de l'article 8, il faut qu'elle remplisse les conditions décrites plus haut mais également qu'elle soit « nécessaire dans une société démocratique ». Selon certains juges strasbourgeois, « Les Etats ne disposent pas d'une latitude illimitée pour assujettir les individus à des mesures de surveillance secrète ou à un système de fichiers secrets. L'intérêt d'un Etat à préserver sa sécurité nationale doit être mis en balance avec la gravité de l'atteinte au droit d'un requérant au respect de sa vie privée. »⁹⁶ Selon Thomas Hammarberg, la balance penche en faveur de ce dernier en ce qui concerne les données sensibles puisqu'il affirme que « la collecte de données sur des individus pour l'unique motif qu'ils ont telle origine raciale, telles convictions religieuses, tel comportement sexuel ou telles opinions politiques ou qu'ils appartiennent à tels mouvements ou organisations qui ne sont pas interdits par la loi devrait être prohibée » sauf si « elle est absolument nécessaire pour les besoins d'une enquête déterminée. »⁹⁷

Dans l'affaire suédoise déjà mentionnée, la circonstance qu'un parti politique « préconise le recours à la violence et à des infractions à la loi pour changer l'ordre social existant », en l'occurrence, le KPML(r), n'a pas été jugée suffisante pour justifier la conservation d'informations sur l'appartenance audit parti. Voici ce que conclut la Cour: « (...) le Gouvernement n'indique aucune circonstance spécifique qui montrerait que les dispositions litigieuses du programme ont trouvé leur expression dans les actes et déclarations des dirigeants ou membres du parti et ont constitué une menace réelle, ou même simplement potentielle, pour la sécurité nationale lorsque les informations ont été divulguées en 1999, soit près de trente ans après la création du parti. Dès lors, les motifs ayant justifié la conservation des informations relatives aux troisième et quatrième requérants, bien que pertinents, ne sauraient être considérés comme suffisants aux fins du critère de nécessité à appliquer sous l'angle de l'article 8 § 2 de la Convention. En conséquence, la conservation des informations communiquées aux requérants concernés en 1999 s'analyse en une ingérence disproportionnée dans l'exercice par les intéressés de leur droit au respect de leur vie privée»⁹⁸.

Ici se pose à nouveau la question de la durée de conservation, de l'absence de modalités de traitement et de gardes-fous solides pour alimenter la BNG et les autres fichiers policiers belges. Dans l'état actuel, il n'est pas interdit de penser que bon nombre d'enregistrements, effectués par prudence, pour éviter le spectre de la « rétention d'information », ne sont en réalité pas nécessaires dans une démocratie qui se respecte.

⁹⁶ Opinion concordante du juge Wildhaber, dans l'affaire Rotaru précitée, à laquelle M. Makarczyk, M. Türmen, M. Costa, Mme Tulkens, M. Casadevall et Mme Weber déclarent se rallier. Il cite les décisions suivantes: arrêt Leander c. Suède du 26 mars 1987, série A no 116, p. 25, § 60 ; voir aussi l'arrêt Klass et autres c. Allemagne du 6 septembre 1978, série A no 28, pp. 21 et 23, §§ 42 et 49 et, mutatis mutandis, l'arrêt Chahal c. Royaume-Uni du 15 novembre 1996, Recueil 1996-V, pp. 1866 1867, § 131, et l'arrêt Tinnelly & Sons Ltd et autres et McElduff et autres c. Royaume-Uni du 10 juillet 1998, Recueil 1998-IV, pp. 1662 1663, § 77.

⁹⁷ Commissaire aux droits de l'homme du Conseil de l'Europe, Lutte contre le terrorisme et protection du droit au respect de la vie privée CommDH/IssuePaper(2008)3, p 10 (se référant au principe 2.4 de la Recommandation n° R(87)15)

⁹⁸ Cour EDH, Segerstedt-Wiberg et autres c. Suède, 6 juin 2006, § 91.

III. 2. Le droit au recours effectif (article 13)

L'article 13 de la Convention est libellé comme suit:

« Toute personne dont les droits et libertés reconnus dans la (...) Convention ont été violés, a droit à l'octroi d'un recours effectif devant une instance nationale, alors même que la violation aurait été commise par des personnes agissant dans l'exercice de leurs fonctions officielles. »

Si un individu se plaint qu'un fichage policier viole l'article 8, il doit pouvoir bénéficier d'un recours interne pour faire respecter son droit à la vie privée. Il n'est pas nécessaire de prouver que l'article 8 a été violé pour y avoir droit. Il suffit d'avoir des griefs que l'on peut estimer « défendables »⁹⁹. Contrairement à l'exigence de l'article 6 de la CEDH, l'article 13 n'impose pas un tribunal indépendant et impartial mais seulement une « l'instance nationale compétente » qui doit « connaître du contenu du grief fondé sur la Convention et (...) offrir le redressement approprié »¹⁰⁰.

Selon la Cour, l'instance doit avoir un pouvoir contraignant à l'égard de la police¹⁰¹. Il n'est pas contestable que la CPVP a un pouvoir contraignant à l'égard de la police puisqu'elle peut lui ordonner de faire rectifier ou effacer des données ainsi que d'insérer des données divergentes par rapport aux données traitées. Elle peut aussi interdire la communication des données¹⁰².

Une question plus importante est de savoir si on doit considérer comme effectif, un recours qui ne peut s'exercer que de manière indirecte. La Cour semble apporter une réponse nuancée. En effet, dans l'affaire Rotaru, elle affirme que : « en matière de surveillance secrète, un mécanisme objectif de contrôle peut être suffisant aussi longtemps que les mesures restent secrètes. Ce n'est qu'une fois les mesures divulguées que des voies de recours doivent s'ouvrir à l'individu »¹⁰³. Il faut noter que, dans le système belge, le recours indirect concerne tant les données secrètes que les informations divulguées (par exemple suite à une procédure pénale). Autrement dit, lorsqu'une personne a acquis la certitude que la police avait traité des données personnelles erronées, elle ne peut presque jamais avoir la garantie que ces données ont été corrigées.

Il n'est pas inutile de reproduire ici des extraits de la Recommandation N° R (87) 15 portant réglementation de l'utilisation des données à caractère personnel dans le secteur de la police, adoptée le 17 septembre 1987 par le Comité des Ministres du Conseil de l'Europe:

« 6.4. L'exercice des droits d'accès, de rectification ou d'effacement ne saurait faire l'objet d'une restriction que dans la mesure où une telle restriction serait indispensable pour l'accomplissement d'une tâche légale de la police »;

« 6.5. Un refus ou une restriction de ces droits devraient être motivés par écrit. La communication de la motivation ne pourrait être refusée que dans la mesure où cela serait indispensable pour l'accomplissement d'une tâche légale de la police. »

⁹⁹ Voir, par exemple, Cour EDH, Çakıcı c. Turquie [GC], no 23657/94, § 112.

¹⁰⁰ Cour EDH, Rotaru précité, § 67.

¹⁰¹ Comm.EDH, Friedl c. Autriche, 19 mai 1994.

¹⁰² Art 43 de l'AR du 13 février 2001 précité.

¹⁰³ Cour EDH, Rotaru précité, § 69 et Klass précité, p. 31, §§ 70-71.

Dans le système belge, la restriction est la règle quasi absolue et est justifiée par la nécessité de respecter la règle du secret de l'instruction et de l'information. Selon le législateur, "il serait paradoxal en effet de permettre aux auteurs, coauteurs ou complices d'infractions pénales de s'informer, avant leur inculpation des éléments de preuve que les autorités judiciaires ont recueilli à leur sujet"¹⁰⁴. Or, cette justification est inadéquate pour toutes les données personnelles recueillies en dehors du cadre d'une enquête pénale.

Selon la Cour, « d'après la jurisprudence de la Convention, un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'Etat peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme »¹⁰⁵. Dans le mécanisme prévu en Belgique, le refus d'accès est généralisé et s'applique dans tous les cas où il n'est pas établi qu'un accès porterait atteinte à l'efficacité du système de surveillance. On peut donc nourrir des doutes très sérieux sur sa compatibilité avec les articles 8 et 13 de la Convention.

Autre question encore plus cruciale: peut-on encore raisonnablement prétendre qu'un recours est effectif «en pratique comme en droit»¹⁰⁶ lorsque son issue reste totalement secrète pour le requérant, comme c'est le cas dans la procédure belge?

Conclusion

Contrairement à ce que d'aucuns pourraient prétendre, le respect de la vie privée et de la protection des données personnelles ne concerne pas seulement ceux qui ont «quelque chose à cacher». Cette observation vaut tout autant, si pas davantage, en matière de fichage policier. On l'a vu, un encodage erroné ou mal interprété peut aboutir à un "faux positif", qui peut générer des mesures gravement attentatoires à d'autres libertés, comme une impossibilité de voyager ou même une arrestation. L'accès à un emploi peut également être refusé sur base d'un fichage erroné. La technologie permet le traitement complexe d'informations sensibles et la gestion d'un flux sans cesse croissant. Le renforcement de la coopération policière et judiciaire pénale, au niveau européen et international multiplie les transferts, donc les risques de traitements problématiques. Par le truchement des principes "de disponibilité" et de "confiance mutuelle", un fichage injustifié peut avoir des conséquences dommageables dans toute l'Union européenne et parfois au-delà.¹⁰⁷

La politique de la "carte blanche" laissée au monde policier pour gérer ses fichiers n'est pas seulement menaçante à l'égard du droit à la vie privée, considéré de manière abstraite. Ce laxisme porte en germe le risque de violation de droits fondamentaux en cascade. Au moment où se discute, en coulisses, un instrument réglant les modalités du traitement des données par la police, et notamment le délai de conservation, l'ensemble des défenseurs des droits humains et des citoyens soucieux de leurs libertés devront se montrer vigilants et "proactifs", lorsque ce dossier reviendra au parlement. Celui-ci serait sans doute bien inspiré de saisir cette occasion pour revoir à la hausse les garanties accordées aux citoyens qui font l'objet de ce fichage afin d'éviter une condamnation de la Belgique par les instances internationales.

¹⁰⁴ Ch., Doc. Parl., 1610/1, 90/91, p. 17 et rapport au Roi présenté par le ministre de la justice de l'époque, Marc Verwilghen, précédant l'AR du 13 février 2001 (MB 13 mars 2001, p 7868).

¹⁰⁵ Cour EDH, Segerstedt-Wiberg et autres c. Suède, 6 juin 2006, § 102, se référant à Klass et autres, § 58, et Leander, § 66.

¹⁰⁶ Cour EDH, arrêt Wille c. Liechtenstein [GC], no 28396/95, § 75.

¹⁰⁷ Voir l'intéressant exemple du couple Moon (de la secte du même nom), sous le coup d'un signalement Schengen pendant plus de 10 ans et donc interdit d'accès dans l'UE qui a introduit différents recours dans différents Etats membres dont la Belgique (Evelien BROUWER, « The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts », CEPS Working document n° 288 / April 2008, <http://www.ceps.eu>)

Annexes

- 1) Extraits de textes juridiques pertinents.
- 2) Déclaration à la CPVP concernant la BNG police administrative
- 3) Courrier-type à adresser à la Commission pour la protection de la vie privée

ANNEXE 1 : EXTRAITS DE TEXTES JURIDIQUES PERTINENTS

Extrait de la loi du 5 août 1992 sur la fonction de police

Sous-section 3. - (De la gestion des informations). <Inséré par L 1998-12-07/31, art. 191; ED : 01-01-2001 >

Art. 44/1. <Inséré par L 1998-12-07/31, art. 191; **En vigueur:** 01-01-2001 > Dans l'exercice des missions qui leur sont confiées, les services de police peuvent recueillir et traiter des données à caractère personnel et des informations relatives notamment à des événements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative et pour l'exécution de leurs missions de police judiciaire conformément aux articles 28bis, 28ter, 55 et 56 du Code d'instruction criminelle.

(En vue d'accomplir leurs missions de police judiciaire et de police administrative, les services de police peuvent recueillir et traiter, selon les modalités déterminées par le Roi, après avis de la Commission de la protection de la vie privée, des données à caractère personnel visées à l'article 6 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.) <L 2001-04-02/34, art. 4, 007; **En vigueur:** 01-01-2001 >

(Ces informations et données ne peuvent être communiquées qu'aux autorités visées à l'article 5, aux services de police (belges ou étrangers), (au Service d'Enquêtes du Comité permanent P, au Service d'Enquêtes du Comité permanent R, (ainsi que par l'Organe de coordination pour l'analyse de la menace,)) à l'inspection générale de la police fédérale et de la police locale ainsi qu'aux services de renseignements et de sécurité (au Comité permanent P et au Comité permanent R) qui en ont besoin pour l'exécution de leurs missions.) (Elles peuvent également être communiquées aux organisations internationales de coopération policière à l'égard desquelles les autorités publiques ou les services de police belges ont des obligations.) <L 2001-04-02/34, art. 4, 007; **En vigueur:** 01-01-2001 > <L 2002-04-26/30, art. 134, 008; **En vigueur:** 30-04-2002 > <L 2003-05-03/59, art. 17, 010; **En vigueur:** 01-07-2003 > <L 2006-07-10/32, art. 16, 013; **En vigueur:** indéterminée et au plus tard : 01-12-2006 >

(Le Roi détermine à quelles autres autorités publiques ces mêmes données et informations peuvent également être communiquées par un arrêté délibéré en Conseil des ministres qui en fixe les modalités après avis de la Commission de la protection de la vie privée.) <L 2002-04-26/30, art. 134, 008; **En vigueur:** 30-04-2002 >

(Le Roi détermine quelles sont les données et informations qui peuvent également être communiquées à LA POSTE, sans préjudice de l'application de l'article 13, § 3, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, en vue du traitement administratif des perceptions immédiates, par un arrêté délibéré en Conseil des Ministres qui en fixe les modalités après avis de la Commission de la protection de la vie privée.) <L 2005-12-27/31, art. 10, 010; **En vigueur:** 09-01-2006 >

Art. 44/2. <Inséré par L 1998-12-07/31, art. 191; **En vigueur:** 01-01-2001> La collecte, le traitement et la transmission des informations et des données visées à l'article 44/1, alinéa 1er, se font conformément à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Ces informations et données doivent présenter un lien direct avec la finalité du fichier et se limiter aux exigences qui en découlent.

(alinéa 2 abrogé) <L 2001-04-02/34, art. 5, 007; **En vigueur:** 01-01-2001>

Des personnes de contact pour la Commission de la Protection de la Vie Privée sont désignées dans les services de police.

(La gestion des structures et moyens techniques informatiques nécessaires pour la banque de données nationale générale visée à l'article 44/4 est assurée par le commissariat général de la police fédérale.) <L 2006-06-20/34, art. 6, 014; **En vigueur:** 01-03-2007>

Art. 44/3. <Inséré par L 1998-12-07/31, art. 191; ED : 01-01-2001> Les informations et les données visées à l'article 44/1, alinéa 1er, relatives aux missions de police administrative sont recueillies et traitées sous l'autorité du ministre de l'Intérieur.

Sans préjudice des compétences des autorités judiciaires, les informations et données visées à l'article 44/1, alinéa 1er, relatives aux missions de police judiciaire sont recueillies et traitées sous l'autorité du ministre de la Justice.

Art. 44/4. <Inséré par L 1998-12-07/31, art. 191; ED : 01-01-2001> Les informations et les données visées à l'article 44/1, alinéa 1er, sont traitées, selon les modalités fixées par le Roi, par arrêté délibéré en Conseil des ministres, dans une banque de données nationale générale, créée (au sein du commissariat général de la police fédérale). (Ces modalités fixent notamment les délais de conservation des informations et des données précitées.) Plusieurs systèmes d'index sont inclus dans cette banque de données. Dans le cadre de ces systèmes d'index, le Roi règle aussi la surveillance (de l'organe de contrôle visé à l'article 44/7) sur l'information judiciaire. <L 2001-04-02/34, art. 6, 007; **En vigueur:** 01-01-2001> <L 0Le Roi fixe, par arrêté délibéré en Conseil des ministres, les conditions sous lesquelles cette banque de données et chacun de ces systèmes d'index sont accessibles et peuvent être consultés par les autorités judiciaires compétentes et les services de police dans le cadre de l'exercice de leurs missions.

Les services de police transmettent d'office et de manière directe à cette banque de données nationale générale les informations et les données visées à l'article 44/1, alinéa 1er.

Les ministres de l'Intérieur et de la Justice, chacun dans le cadre de ses compétences, déterminent, sur avis conforme de l'organe de contrôle visé à l'article 44/7, les catégories d'informations et de données qui n'exigent pas une transmission.

Art. 44/5. <Inséré par L 1998-12-07/31, art. 191; **En vigueur:** 01-01-2001> Lorsque, dans le cadre de l'exercice de leurs missions de police administrative, les services de police acquièrent connaissance d'informations intéressant l'exercice de la police judiciaire, ils en informent sans délai ni restriction les autorités judiciaires compétentes.

Lorsque dans le cadre de l'exercice de leurs missions de police judiciaire, les services de police acquièrent la connaissance d'informations intéressant l'exécution de la police administrative et qui peuvent donner lieu à des décisions de police administrative, ils en informent les autorités administratives compétentes, sauf si cela peut porter atteinte à l'exercice de l'action publique, mais sans préjudice des mesures indispensables à la protection des personnes.

Art. 44/6. <Inséré par L 1998-12-07/31, art. 191; En vigueur : 01-01-2001> Dans l'exercice de leurs missions de police judiciaire, les services de police communiquent les informations et les données visées à l'article 44/1, alinéa 1er, aux autorités judiciaires compétentes, conformément aux articles 28bis, 28ter, 55 et 56 du Code d'instruction criminelle.

Art. 44/7. <Inséré par L 1998-12-07/31, art. 191; En vigueur : 01-01-2001> Il est créé un organe de contrôle sous l'autorité du ministre de l'Intérieur et du ministre de la Justice, chargé du (contrôle du traitement des informations et des données visées à l'article 44/1, alinéa 1er). Cet organe de contrôle a un accès illimité à toutes les informations et les données conservées dans cette banque de données. <L 2001-04-02/34, art. 7, 007; **En vigueur:** 01-01-2001>

Il est particulièrement chargé de contrôler le respect des règles d'accès à la banque de données nationale générale et de transmission à cette banque des données et informations visées à l'article 44/1, alinéa 1er.

Sans préjudice des dispositions visées à l'article 44/4, les services de police peuvent, dans des circonstances particulières, créer des banques de données. La création de toute banque de données par les services de police doit préalablement être communiquée à cet organe de contrôle. Toutes les informations et les données de ces banques de données sont communiquées à la banque de données nationale générale visée à l'article 44/4, alinéa 1er, sauf accord de l'organe de contrôle sur une demande de non transmission. Toutes les compétences attribuées à l'organe de contrôle par le présent article s'appliquent intégralement à ces banques de données. Dans les conditions déterminées par le Roi, par arrêté délibéré en Conseil des ministres, ces banques de données sont accessibles et consultables par les autorités compétentes, chacune dans le cadre de ses compétences, et par les services de police dans le cadre de l'exercice de leurs missions.

Afin d'accomplir ses missions de contrôle, cet organe a un droit d'accès illimité aux locaux dans lesquels et pendant le temps où les fonctionnaires de police y exercent leurs fonctions.

Cet organe est présidé par un magistrat fédéral. Ce magistrat est désigné par le ministre de la Justice et le ministre de l'Intérieur, (sur proposition du procureur fédéral). Il agit, pendant la durée de sa désignation, de manière indépendante à l'égard du parquet fédéral. Pour le surplus, cet organe est composé d'un membre de la police locale, d'un membre de la police fédérale et d'un expert qui sont désignés par les ministres de l'Intérieur et de la Justice. (En cas d'absence, le président et les membres ont en outre chacun un suppléant désigné conformément aux procédures respectives des membres effectifs.) <L 2001-04-02/34, art. 7, 007; **En vigueur:** 01-01-2001>

L'organe de contrôle agit d'initiative ou à la demande des autorités judiciaires ou administratives, du ministre de la Justice ou du ministre de l'Intérieur, dans les conditions fixées par le Roi, par arrêté délibéré en Conseil des ministres.

Lorsque le contrôle a eu lieu au sein d'une police locale, l'organe de contrôle en informe le bourgmestre ou le collège de police et lui adresse son rapport.

Lorsque le contrôle concerne des renseignements et des données concernant l'exécution des missions de police judiciaire, le rapport y relatif qui est établi par l'organe de contrôle est également transmis au procureur du Roi.

Cet organe de contrôle bénéficie de l'appui administratif et logistique de l'inspection générale de la police fédérale et de la police locale et peut, pour l'exécution de sa mission, requérir l'assistance de cette inspection.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, les règles relatives au statut des membres de cet organe de contrôle (et de leurs suppléants) de manière à garantir leur indépendance. <L 2001-04-02/34, art. 7, 007; **En vigueur**: 01-01-2001>

Art. 44/8. <Inséré par L 1998-12-07/31, art. 191; **En vigueur**: 01-01-2001> En dérogation à l'article 44/4, la transmission visée à l'article 44/4, alinéa 3, est différée lorsque et aussi longtemps que le magistrat compétent, avec l'accord du (procureur fédéral), estime que cette transmission peut compromettre l'exercice de l'action publique ou la sécurité d'une personne. <L 2001-04-02/34, art. 8, 007; **En vigueur**: 01-01-2001>

Art. 44/9. <Inséré par L 1998-12-07/31, art. 191; En vigueur : 01-01-2001> Les fonctionnaires de police chargés de la gestion de la banque de données nationale générale visée à l'article 44/4, alinéa 1er, sont désignés après l'avis de l'organe de contrôle visé à l'article 44/7. Aucune promotion, nomination ou mutation ne peut leur être octroyée que sur initiative ou de l'accord du ministre compétent et après avis de cet organe de contrôle. Les modalités en sont déterminées par le Roi.

A l'égard de ces fonctionnaires de police, une procédure disciplinaire pour des faits commis pendant la durée de leur désignation ne peut être intentée que de l'accord ou sur ordre du ministre compétent. L'avis de l'organe de contrôle est recueilli pour les procédures disciplinaires qui ne sont pas ordonnées par le ministre.

La banque de données nationale générale visée à l'article 44/4, alinéa 1er, est gérée au sein d'un service placé sous la direction d'un chef de service et d'un chef de service adjoint. Un des deux est membre de la police fédérale et l'autre appartient à la police locale. Les modalités de leur désignation sont arrêtées par le Roi.

Art. 44/10. <Inséré par L 1998-12-07/31, art. 191; En vigueur : 01-01-2001> Les mesures d'exécution visées aux articles (...)44/4, alinéa 2 et 44/7, alinéas 3 et 9, sont prises après avis de la Commission de la Protection de la Vie privée, sauf en cas d'urgence. <L 2001-04-02/34, art. 9, 007; **En vigueur**: 01-01-2001>

Art. 44/11. <Inséré par L 1998-12-07/31, art. 191; ED : 01-01-2001> Tout fonctionnaire de police qui retient, sciemment et volontairement des informations et des données présentant un intérêt pour l'exécution de l'action publique ou le maintien de l'ordre public et s'abstient de les transmettre à la banque de données nationale générale, conformément à l'article 44/4, alinéa 3, sera puni d'un emprisonnement d'un mois à six mois et d'une amende de vingt-six à cinq cents francs, ou d'une de ces peines seulement.

Les dispositions du livre Ier du Code pénal, en ce compris le chapitre VII et l'article 85, sont d'application à cette infraction.

Article 13 de la loi du 8 décembre 1992 sur la protection de la vie privée

Art. 13. Toute personne justifiant de son identité a le droit de s'adresser sans frais à la Commission de la protection de la vie privée pour exercer les droits visés aux articles 10 et 12 à l'égard des traitements de données à caractère personnel visés à l'article 3, §§ 4, 5 et 6. Le Roi détermine, après avis de la Commission de la protection de la vie privée et par arrêté délibéré en Conseil des ministres, les modalités d'exercice de

ces droits. La Commission de la protection de la vie privée communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires. Toutefois, le Roi détermine, après avis de la Commission de la protection de la vie privée, par arrêté délibéré en Conseil des ministres, quelle information peut être communiquée à l'intéressé lorsque la demande de celui-ci porte sur un traitement de données à caractère personnel géré par des services de police en vue de contrôles d'identité.

Extrait de l'AR du 13 février 2001

CHAPITRE VI. - Exercice du droit visé à l'article 13 de la loi.

Art. 36. Le présent chapitre détermine la procédure relative aux demandes introduites en vertu de l'article 13 de la loi.

Art. 37. La demande est introduite par la personne concernée auprès de la Commission par courrier daté et signé. La demande contient : le nom, le prénom, la date de naissance, la nationalité de la personne concernée, ainsi qu'une photocopie de la carte d'identité, du passeport ou du document qui en tient lieu.

La demande contient, en outre et dans la mesure où le demandeur dispose de ces informations :

- la désignation de l'autorité ou du service concerné;
- tous les éléments pertinents concernant les données contestées, tels que leur nature, les circonstances ou l'origine de la prise de connaissance des données contestées, ainsi que les rectifications éventuellement souhaitées.

Art. 38. La Commission peut demander, à la personne concernée, tous renseignements complémentaires qu'elle estime utile.

Art. 39. A défaut des éléments mentionnés aux articles 37 et 38 du présent arrêté, la demande pourra être considérée comme irrecevable.

Art. 40. La demande est irrecevable si elle est introduite dans un délai inférieur à un an à compter de la date d'envoi de la précédente réponse de la Commission concernant les mêmes données et les mêmes services.

Il peut être dérogé à ce délai, à charge pour la personne intéressée d'exposer, dans sa demande, les motifs justifiant cette dérogation.

Art. 41. Lorsque la demande est considérée comme irrecevable, la personne concernée en est avisée par courrier.

Le courrier mentionne que si la personne concernée le souhaite, elle est entendue, éventuellement assistée de son conseil.

Art. 42. Le contrôle, exercé auprès du service concerné, est effectué par le président de la Commission ou par un ou plusieurs membres désignés par lui.

Le contrôle des traitements de données à caractère personnel, visés à l'article 3, § 5, 1°, de la loi, est effectué par des magistrats désignés par la Commission en son sein.

Le président et les membres, qui effectuent le contrôle, peuvent se faire assister ou représenter par un ou plusieurs membres du secrétariat de la Commission.

Art. 43. A l'occasion du contrôle exercé auprès du service concerné, la Commission effectue ou ordonne toute vérification qu'elle estime utile.

A l'occasion du contrôle exercé auprès du service concerné, visé à l'article 3, § 5, de la loi, elle peut faire rectifier ou effacer des données, ainsi que insérer des données divergentes par rapport aux données traitées par le service concerné. Elle peut interdire la communication des données.

A l'occasion du contrôle exercé auprès du service concerné, visé à l'article 3, § 4, de la loi, elle recommande les mesures qu'elle estime nécessaire. Elle motive ses recommandations.

Art. 44. A l'issue de ces vérifications, le service concerné notifie, par écrit, à la Commission, les suites qui y ont été réservées.

Art. 45. La Commission répond, par courrier, à la demande de la personne concernée dans un délai de trois mois à compter de la notification prévue à l'article 44 du présent arrêté.

Art. 46. Lorsque la demande de la personne concernée se rapporte à un traitement de données à caractère personnel, géré par un service de police, en vue d'un contrôle d'identité, la Commission communique à la personne concernée que les vérifications nécessaires ont été effectuées.

Le cas échéant, la Commission fournit, à la personne concernée, après avis du service concerné, toute autre information qu'elle estime appropriée.

ANNEXE 2: DÉCLARATION À LA CPVP CONCERNANT LA BNG POLICE ADMINISTRATIVE

PARTIE 1. Responsable du traitement



Nom (ou dénomination de la personne morale, de l'association de fait ou de l'administration publique)

Le Ministre de l'Intérieur

Adresse:

de la loi 2

1000 BRUXELLES

Belgique

Statut juridique du responsable de traitement

- *Autorité publique*
- *Service de police*

PARTIE 2. Le traitement



1. Dénomination du traitement

Banque de données Nationale Générale-traitements de police administrative

2. Finalité ou ensemble de finalités liées pour lesquelles des données sont traitées

- Missions de police administrative

3. Catégories de données traitées

- Données d'identification (nom, adresse, tél., ...)
- Données d'identification électronique (adresses IP, cookies, ...)
- Données de localisation électronique (GSM, GPS, ...)
- Données d'identification biométrique
- Caractéristiques personnelles (âge, sexe, état civil, ...)
- Affiliations
- Profession et emploi
- Enregistrements d'images
- Numéro du Registre national/numéro d'identification de la sécurité sociale
- Données raciales ou ethniques
- Opinions politiques
- Convictions religieuses ou philosophiques
- Condamnations et peines
- Mesures judiciaires
- Sanctions administratives

4. La (les) base(s) légale(s) ou réglementaire(s)

Loi, décret ou ordonnance, AR ou arrêté du 05/08/1992

Titre *loi sur la fonction de police, articles 44/1 et suivants*

Loi, décret ou ordonnance, AR ou arrêté du 08/12/1992

Titre *loi relative à la protection de la vie privée*

5. Catégorie(s) de destinataires et de données qui peuvent être fournies

Justice et services de police

- Données d'identification (nom, adresse, tél., ...)
- Données d'identification électronique (adresses IP, cookies, ...)
- Données de localisation électronique (GSM, GPS, ...)
- Données d'identification biométrique
- Caractéristiques personnelles (âge, sexe, état civil, ...)
- Affiliations
- Condamnations et peines
- Mesures judiciaires
- Sanctions administratives
- Profession et emploi
- Numéro du Registre national/numéro d'identification de la sécurité sociale
- Données raciales ou ethniques
- Opinions politiques
- Convictions religieuses ou philosophiques
- Enregistrements d'images

6. Quelles sont les mesures de sécurité prises lors de la communication des données à des tiers ?

- Mesures techniques (par exemple : cryptage, mots de passe, ...)

7. Comment les personnes concernées sont-elles informées de l'enregistrement de leurs données ?

Les données à caractère personnel sont traitées sans que la personne concernée doive en être informée.

- Je suis exempté(e) d'information, en application de l'art. 3, §5 LVP, le traitement est géré en vue de l'exercice de :
Partie applicable de la disposition: 3§5, 2° LVP

8. A qui les personnes concernées peuvent-elles s'adresser afin d'exercer leurs droits ?

Le droit d'accès de la personne concernée à ses données ainsi que le droit de rectification et de suppression sont prévus aux articles 10-12 de la LVP

Nom et prénoms (et/ou nom du service)

la commission de la protection de la vie privée

Adresse:

haute 139

1000 BRUXELLES

Téléphone +32 2 213 85 40

Téléfax +32 2 213 85 65

Email *commission@privacy.fgov.be*

9. Mesures particulières pour l'exercice des droits

La commission de la protection de la vie privée dispose d'un point de contact au sein de la direction de la Banque de données Nationale Générale des services de police. Ce point de contact est chargé de fournir à la commission les éléments qu'elle lui demande en vertu de l'article 13 de la loi vie privée

10. Durée de conservation prévue

<i>Données d'identification (nom, adresse, tél., ...)</i>	<i>5 Années</i>
<i>Données d'identification électronique (adresses IP, cookies, ...)</i>	<i>5 Années</i>
<i>Données de localisation électronique (GSM, GPS, ...)</i>	<i>5 Années</i>
<i>Données d'identification biométrique</i>	<i>5 Années</i>
<i>Caractéristiques personnelles (âge, sexe, état civil, ...)</i>	<i>5 Années</i>
<i>Affiliations</i>	<i>5 Années</i>
<i>Condamnations et peines</i>	<i>5 Années</i>
<i>Mesures judiciaires</i>	<i>5 Années</i>
<i>Sanctions administratives</i>	<i>5 Années</i>
<i>Profession et emploi</i>	<i>5 Années</i>
<i>Numéro du Registre national/numéro d'identification de la sécurité sociale</i>	<i>5 Années</i>
<i>Données raciales ou ethniques</i>	<i>5 Années</i>
<i>Opinions politiques</i>	<i>5 Années</i>
<i>Convictions religieuses ou philosophiques</i>	<i>5 Années</i>
<i>Enregistrements d'images</i>	<i>5 Années</i>

*Si des durées de conservation particulières sont d'application, veuillez les préciser.
pour les exceptions, voir annexe 1*

11. Description générale des mesures de sécurité

Mesures générales prises en vue d'assurer la confidentialité et la sécurité du traitement (art. 16 LVP).

Service de sécurité

Mesures de prévention de risques

Système de backup

Sécurisation et contrôle des bâtiments, locaux et appareils

Sécurisation de l'accès au système

Système d'authentification

Système de logging

Mesures par contrat vis-à-vis

Du personnel

Code de conduite (complétez le cadre ci-dessous)

déontologie, respect du secret professionnel

Mesures de sécurité supplémentaires à prendre lors d'un traitement de données à caractère personnel visées aux articles 6 à 8 LVP (art. 25 et 26 AR)

*** TRAITEMENT DE DONNEES SENSIBLES, RELATIVES A LA SANTE OU JUDICIAIRES VISEES AUX ARTICLES 6 à 8 LVP**

En vertu de l'art. 25 AR, vous devez disposer d'une liste actuelle des catégories désignées de personnes qui peuvent consulter ces données à caractère personnel

Où la Commission peut-elle consulter cette liste ? (art. 25,2°AR)

Nom et prénoms (ou dénomination de la personne morale, de l'association de fait ou de l'administration publique)

Marc Vandendriessche (Direction de la Banque de données Nationale Générale)

Adresse:

Fritz Toussaint 8

1050 BRUXELLES (IXELLES)

Téléphone +32 2 642 78 39

Téléfax +32 2 642 76 38

Email *marc.vdd@skynet.be*

*** TRAITEMENT DES DONNEES SENSIBLES OU RELATIVES A LA SANTE, VISEES AUX ARTICLES 6 ET 7 LVP, QUE VOUS EFFECTUEZ SUR BASE DU CONSENTEMENT ECRIT DE LA PERSONNE CONCERNEE**

Traitez-vous des données sensibles ou relatives à la santé, visées aux articles 6 et 7 LVP, sur base du consentement écrit de la personne concernée ?

Oui

Où la Commission peut-elle consulter cette liste ?

Nom et prénoms (ou dénomination de la personne morale, de l'association de fait ou de l'administration publique)

X

Adresse:

X

X X

Téléphone *X*

Téléfax *X*

Email *X*

12. Données transmises à l'étranger

Tous les pays de l'Union européenne

- Données d'identification (nom, adresse, tél., ...)
- Données d'identification électronique (adresses IP, cookies, ...)
- Données de localisation électronique (GSM, GPS, ...)
- Données d'identification biométrique
- Caractéristiques personnelles (âge, sexe, état civil, ...)
- Affiliations
- Condamnations et peines
- Mesures judiciaires
- Sanctions administratives
- Profession et emploi
- Numéro du Registre national/numéro d'identification de la sécurité sociale
- Données raciales ou ethniques
- Opinions politiques
- Convictions religieuses ou philosophiques
- Enregistrements d'images

Tous les pays hors Union européenne

- Données d'identification (nom, adresse, tél., ...)
- Données d'identification électronique (adresses IP, cookies, ...)
- Données de localisation électronique (GSM, GPS, ...)
- Données d'identification biométrique
- Caractéristiques personnelles (âge, sexe, état civil, ...)
- Affiliations
- Condamnations et peines
- Mesures judiciaires
- Sanctions administratives
- Profession et emploi
- Numéro du Registre national/numéro d'identification de la sécurité sociale
- Données raciales ou ethniques
- Opinions politiques
- Convictions religieuses ou philosophiques
- Enregistrements d'images

Dans le cas d'un transfert de données à caractère personnel vers un pays n'assurant pas le niveau de protection adéquat, et après vérification de la liste établie par la Commission européenne, indiquez, en vertu de l'article 22 LVP, la raison permettant ce transfert:

- *Nécessaire ou juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice*

ANNEXE 3: LETTRE TYPE DROIT D'ACCÈS INDIRECT

CPVP
Rue Haute, 139
1000 BRUXELLES

Mon prénom et mon nom
Mon adresse
Mon adresse e-mail

Concerne : accès indirect à mes données à caractère personnel

lieu et date

Madame, Monsieur

Je vous envoie par la présente une demande d'accès indirect à mes données (veuillez sélectionner une des possibilités ci-dessous):

- ☐ dans la base de données de (nom de l'instance concernée si elle est connue);
- ☐ dans la base de données de la police fédérale;
- ☐ dans la base de données de la Sûreté de l'État;
- ☐ dans la base de données d'une autre instance que je ne connais pas;
- ☐ dans le Système d'Information Schengen.

Etant donné que l'article 13 de la Loi vie privée stipule que je ne peux consulter les données conservées par ce(s) responsable(s) qu'indirectement, je demande à la Commission de la protection de la vie privée (CPVP) de le faire à ma place. Je suis parfaitement conscient que la CPVP me communiquera, en principe, uniquement qu'elle a effectué les vérifications nécessaires.

Conformément à l'article 37 de l'Arrêté royal portant exécution de la Loi vie privée, je vous joins aussi les données suivantes:

- ma date de naissance :
- ma nationalité :
- tous les éléments pertinents (p. ex. la nature des données, les circonstances du traitement des données, les raisons pour lesquelles vous voulez prendre connaissance de vos données, une éventuelle contestation ou rectification des données):
.....
.....
.....

A titre de preuve de mon identité, je joins à la présente une copie de ma carte d'identité (ou de mon passeport ou autre document y assimilé).

Cordiales salutations

Signature

Annexe: copie de ma carte d'identité / passeport / document y assimilé

NUT EN BEPERKINGEN VAN DE BEROEPEN MET BETREKKING TOT DE FICHAGE VAN DE BURGER DOOR DE POLITIE

Vertaling

«La garantie des droits de l'Homme et du Citoyen nécessite une force publique : cette force est donc instituée pour l'avantage de tous, et non pour l'utilité particulière de ceux auxquels elle est confiée.»

(artikel 12 van de 'Déclaration des droits de l'homme et du citoyen' van 1789²)

Inleiding

'Betrokkene is bij onze diensten ook bekend voor feiten als...(naar keuze: nachtlawaai, verdovende middelen, prostitutie, zakkenrollen)'. Advocaten strafrecht treffen regelmatig dat soort raadselachtige vermeldingen aan in een proces verbaal, zelfs als hun cliënt een blanco strafregister heeft. "Reeds gekend door onze diensten" is een steeds weerkerende zin in de politie retoriek, een soort label waardoor beschuldigingen geloofwaardiger moeten lijken terwijl er geen enkel concreet element voorradig is om ze te staven. Dat is de macht van de gegevensbestanden van de politie: op het juiste moment een inlichting bovenhalen, zelfs al is er geen verband met de lopende zaak. Ze zal aan de verdachte een soort label geven waar de rechter, op z'n minst onbewust, misschien gevoelig aan is.

In de vervolging van misdaad en delicten (opdracht van gerechtelijke politie) en haar voorzorgsmaatregelen om de openbare orde te handhaven (opdracht van de administratieve politie), is politiewerk natuurlijk ondenkbaar zonder het vergaren en behandelen van gevoelige informatie. Maar voor de repressieve diensten in het bijzonder is het motto " informatie is macht" uiterst belangrijk. De politionele appetijt voor informatie neigt naar een onverzadigbare gulzigheid. Sedert lang komen repressieve gegevensbestanden en individuele rechten onderling in conflict³. Maar meerdere factoren hebben de laatste tijd dit spanningsveld versterkt: nauwere samenwerking tussen politie en inlichtingsdiensten⁴, het organiseren van gegevensbestanden in het kader van de Europese Unie⁵, groeiende uitwisseling van informatie op internationaal vlak... Deze bijdrage beperkt zich tot de gegevensbestanden van de Belgische politiediensten en haalt de kwestie van deze spanning kort aan in een louter praktisch perspectief. Zou een vorm van democratische of burgerlijke controle over de politionele gegevensbestanden een absurd idee zijn?

² Tekst te vinden op: <http://www.assemblee-nationale.fr/histoire/dudh/1789.asp>

³ Rond 1900 heeft de Franse generaal André 25.000 fiches over politieke en religieuze overtuigingen van de officiers met vermeldingen zoals: « VLM » voor « va à la messe », « grand avaleur de bon Dieu », « rallié à la République, n'en porte pas moins un nom à particule », « a qualifié les maçons et les républicains de canailles, de voleurs et de traîtres », « vit maritalement avec une femme arabe » en nog « vieille peau fermée à nos idées ». (Assemblée nationale, Rapport d'information n° 1548 sur les fichiers de police, déposé par Delphine BATHO et Alain BENISTI, 24 mars 2009, p 12.)

⁴ De fichage door inlichtingendiensten wordt hier niet besproken. Zie: Tom DECAIGNY, Paul DE HERT, « De Wet bijzondere methoden inlichtingen- en veiligheidsdiensten (BIM) », Ad Rem, 1/2009, pp. 24-35. Het wetsontwerp werd intussen door de Senaat aangenomen op 21 januari 2010. Zie doc. Parl. K. N° 52 / 2128 op de website www.dekamer.be

⁵ Het beste voorbeeld is het Schengeninformatiesysteem (SIS): oorspronkelijk bedoeld voor de grenscontroles, maar nu uitgebreid om Europese burgers te controleren. Zie het zeer interessante boek van Evelien BROUWER, Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System, Leiden/Boston: Martinus Nijhoff Publishers, series Immigration and Asylum Law and Policy in Europe, 2008.

Bepaalde episodes uit de recente geschiedenis van de politie tonen aan dat die controle er niet is. De mechanismen ter informatie en de mogelijkheden voor de burger om ervan gebruik te kunnen maken voor controle van deze persoonlijke gegevens zijn niet bepaald overweldigend. (II). Men kan zich terecht vragen stellen over de overeenstemming van deze zwakke garanties met hogere normen die de privacy beschermen zoals het Europees verdrag van de Rechten van de Mens.

I. Inkijkrecht van de burger in de gegevensbestanden van de politie: subversief idee of democratische noodzaak?

Na studie van meerdere voormalige of meer recente fenomenen op Belgisch, Europees of internationaal vlak, zal ik de noodzaak verduidelijken aan een inkijkrecht in de gegevensbestanden van de politie. We beperken ons hier tot een klein overzicht.

I. 1. 'Ethnisch profileren': slechts enkele "uitschuivers" of een belangrijke trend?

Midden de jaren 1990 zette de rijkswacht, geïnspireerd door methodes uit omliggende landen⁶, een bizarre operatie op poten, "Rebel" genaamd, die enkel "Turkse" criminele organisaties beoogde met als doel "de echte verantwoordelijken van de heroïnehandel in België te identificeren". In 1996 had de pers een verband gelegd tussen de massale fichering van Turkse onderdanen en van Belgen van Turkse oorsprong, en een samenwerkingsakkoord tussen de Belgische rijkswacht en het Turkse ministerie van binnenlandse zaken. De verklaring van de toenmalige minister van justitie voor het parlement was allesbehalve overtuigend: het ging over de registratie van bepaalde leden van de Turkse gemeenschap om zo de "kaïds" van de drughandel te kunnen identificeren, vanuit de wetenschap dat de heroïne handel in België in handen was van het Turkse milieu. Een senator stelt ironisch: 'Gaat men dan een screening bestellen van alle West-Vlamingen als men merkt dat vele fraudeurs in de textielsector en hormonentrafikanten uit West-Vlaanderen komen?'⁷ Het Comité P, het orgaan dat de politiediensten controleert, krijgt de opdracht deze zaak uit te spitten. Het zal 5 jaar duren omop enkele details na, dezelfde uitleg te krijgen. Het ging er dus over om persoonlijke gegevens van 90.330 mensen uit de "gemeenschap", te verzamelen, die vervolgens anoniem te maken, om zo een idee te krijgen over verschillende "socio-demografische" elementen betreffende de Turkse gemeenschap in België: aanwezigheid per regio, lokalisatie van grote groepen van de bevolking, leeftijdspiramide.... Op basis van deze gegevens zou de rijkswacht "potentiële criminelen" (5.185 personen teruggebracht tot 61 personen na selectie qua profiel, op basis van criteria uitgewerkt in functie van profielanalyses van beruchte criminelen). Volgens het Comité P is er niets gebeurd dat niet wettelijk is en de operatie werd gerechtvaardigd door het doel namelijk de "identificatie van de werkelijke verantwoordelijken voor de heroïnehandel in België"⁸.

⁶ Verenigde Koninkrijk (Centurionproject), Nederland (IRT) en Duitsland (Anadalou), volgens het jaarverslag 2001 van het Comité P, p 40, www.comitep.be.

⁷ Zie opmerkingen van Boutmans en Erdman, Doc. Parl., Senaat, 1995-1996, Annales de la réunion publique de commission, réunion de la commission de la justice du 3 juillet 1996, pp.303-312 en Compte rendu analytique du 3 juillet 1996, Sénat, réunions publiques de commission, pp.202-206.

⁸ Comité P, jaarverslag 2001, p 40.

Spijtig genoeg is de oorspronkelijke vraagstelling onbeantwoord gebleven: waarom was het nodig om persoonlijke gegevens van 90 000 personen te verzamelen om enkele tientallen potentiële criminelen te identificeren? Waarom kon men de aandacht niet richten op reeds geïdentificeerde milieus? Is er nagegaan of de gegevensanalyse van die 90 000 personen wel degelijk anoniem werd gemaakt en slechts “socio-demografische” elementen bevatte? En tenslotte, hoeveel ‘kaïds’ werden er geïdentificeerd en veroordeeld dank zij operatie “Rebel”?

Tot op heden is daarover niets bekend. Maar volgens het Comité P is er geen enkele reden tot ongerustheid en trouwens dit type projecten zijn vandaag schering en inslag⁹.

Sindsdien hebben operaties waarbij etnisch geprofileerd wordt (“ethnic profiling”) de wind mee in landen die betrokken zijn bij de antiterrorisme strijd. Tussen 2001 en 2003 heeft de Duitse politie gevoelige informatie over ongeveer 8,3 miljoen mensen met een gelijkaardig profiel als die van de ‘cel Hamburg’, waarvan enkele daders van de aanslag van 11 september 2001 deel uitmaakten, verzameld. Er werd een gegevensbestand van ongeveer 32.000 potentiële ‘slapende’ terroristen aangelegd : mannen tussen 18 en 40 jaar, (ex)studenten, moslims of mensen afkomstig uit een land waar islam in de meerderheid is.

Na inzameling en groepering van talrijke andere gegevens met name bij universiteiten, instellingen van sociale zekerheid, plaatselijke autoriteiten, heeft de politie zich uiteindelijk op 1.689 personen gefocust. Deze werden diepgaander onderzocht: ondervraging van hun omgeving, soms van hun werkgever, andere maatregelen tot en met het af luisteren van telefoon. Resultaat: nul (niemand was redelijkerwijs verdacht en nog minder veroordeeld voor terrorisme)¹⁰. Men kan stellen dat de inefficiëntie van deze werkwijze in de strijd tegen de criminaliteit is aangetoond. Een inefficiënte methode maar ver van ongevaarlijk. Het Duitse Grondwettelijk Hof heeft het procédé krachtig veroordeeld en noemt het stigmatiserend voor een ganse religieuze gemeenschap met risico op discriminatie zowel persoonlijk als beroepsmatig¹¹.

1.2. Een erg relatief verbod van politieke fichage

In het begin van de jaren 1980, barste een schandaal los rond de Belgische rijkswacht die nauwgezet politieke- en vakbondsmilitanten in een kaartensysteem had opgenomen op de sindsdien beruchte “microfiches B”¹². In principe is het verzamelen van gegevens aangaande de politieke overtuiging, de filosofische of religieuze opvattingen, het lidmaatschap van een vakbond, de ras- of etnische origine, of het seksuele leven van personen, strikt verboden¹³. De politie beschikt evenwel over een uitzondering op dit verbod en kan dus dit soort belangrijke gegevens verzamelen. Volgens welke modaliteiten? Dat blijft vrij vaag¹⁴. In de praktijk stelt men niettemin vast dat politieke fichage in de mode is.

⁹ Comité P, jaarverslag 2001, p 42. www.comitep.be

¹⁰ Open Society Justice initiative, Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory, p 68-69. Originele versie in het Engels: http://www.soros.org/initiatives/justice/focus/equality_citizenship/articles_publications/publications/profiling_20090526/profiling_20090526.pdf.

¹¹ Volgens het Duitse Grondwettelijk Hof kan de algemene situatie na 9/11 dergelijke inbreuken op de privacy niet rechtvaardigen. Enkel aanwijzingen van concrete feiten van voorbereiding of betrokkenheid van terroristische misdrijven zouden die inbreuken kunnen rechtvaardigen. Beslissing van 4 april 2006, geciteerd door Open Society Justice initiative, Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory, p 70, en ook door Olivier DE SCHUTTER en Julie RINGELHEIM, « Ethnic Profiling: A Rising Challenge for European Human Rights Law », The Modern Law Review, 2008, 71 (3), p 376.

¹² Zie hierover: Colette BRAECKMAN, Marc DE KOCK, Les libertés malades du pouvoir, Bruxelles, Vie Ouvrière, 1980, p 231.

¹³ Art. 6 van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (hierna « privacywet ») “ § 1. De verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de verwerking van persoonsgegevens die het seksuele leven betreffen, is verboden.” De tweede paragraaf van deze bepaling voorziet veel derogaties waaronder de toestemming van de betrokken persoon en “l) wanneer de verwerking van de persoonsgegevens om een andere belangrijke reden van publiek belang door een wet, een decreet of een ordonnantie wordt toegelaten.”

¹⁴ Art. 44/1 al. 2 WPA voorziet dat de modaliteiten moeten door een KB geregeld worden. Ten tijde van het verschijnen van dit artikel (februari 2010) was er nog geen KB aangenomen. De huidige optie is een wetswijziging (wordt voor de zomer van 2010 verwacht).

In 2005 werd het bestaan van een lijst getiteld „extremistische en terroristische groeperingen in Antwerpen” die door de politie van Antwerpen werd opgesteld, openbaar gemaakt. Deze lijst bevatte talrijke gerespecteerde verenigingen, met name pacifistische en interculturele (Hand in hand, vaka, Forum voor vredesactie) en communautaire, gekwalificeerd als „etnische groeperingen” (Verenigen Van Turkse Verenigingen, Verenigen van moskeeën in islamitische verenigingen)¹⁵. Onder de rubriek „extreem links organisaties” , vond men de identiteiten (soms slecht gespeld) van vier advocaten, die in verband gebracht werden met „advocaten voor het volk (Progressief (sic) Lawyers Network)”, evenals het adres van twee kabinetten in Antwerpen. Tot de dag van vandaag weten zij nog steeds niet voor welke redenen zij als “extremisten” of “terroristen” werden gekwalificeerd.

1.3. De Algemene Nationale Gegevensbank (ANG) van de geïntegreerde politie

De huidige Belgische politiestructuur¹⁷ wordt diepgaand bepaald door het trauma van de zaak Dutroux, die werd gekenmerkt door de oorlog van de verschillende politiediensten en van het achterhouden van informatie wat bijdroeg tot het fiasco van het onderzoek over de verdwijning kinderen¹⁸.

1. 3.1. Een « concreet belang » op zoek naar een precieze definitie

Voortaan moet elke informatie die een “concreet belang”¹⁹ heeft voor de rechterlijke of administratieve taken van de politie, opgeslagen worden in een algemene nationale gegevensbank (ANG), een soort “centrale referentiek”²⁰, toegankelijk voor alle politieagenten en magistraten van het land²¹. Het begrip „concreet belang” wordt niet door de wet gedefinieerd. Volgens een richtlijn van 2002 is “de politieambtenaar de essentiële filter die oordeelt of de informatie waarvan hij kennis heeft genomen, voldoende belangrijk is om in een informatierapport te worden geregistreerd”²². Men kan zich afvragen of “een filter” die enkel rust op de beoordelingsmacht van de politieagent werkelijk zijn rol zal spelen. De voornoemde richtlijn geeft: “enkele voorbeelden van informatie die een concreet belang vertonen voor de uitoefening van de politieopdrachten”, met name:

- “• het plegen van een hold-up in een bankinstelling (concrete informatie van gerechtelijke politie);
- de door een tipgever verstrekte informatie van plannen om een diefstal gewapenderhand te plegen in een apotheek (niet concrete informatie van gerechtelijke politie);

¹⁵ Volgens de minister van Binnenlandse zaken van toen ging het enkel om informatie die de drukkingsgroep zelf geeft, of te vinden is in open bronnen, of wanneer het gaat om “te volgen groeperingen” (Vragen en Antwoorden, Bull. , Senaat , 2005-2006, nr. 3-58, vraag nr. 3-2874 van Mevr. Bousakla van 9 juni 2005.

¹⁷ De belangrijkste juridische bronnen zijn de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus en, wat sommige aspecten waaronder de ANG betreft, de wet van 5 augustus 1992 op het politieambt (hierna « WPA »).

¹⁸ In 1995 had de rijkswacht een geheime operatie georganiseerd om toezicht te houden op de pedofiel Marc Dutroux, die belangrijke gegevens opleverde. Deze dienst heeft nagelaten om cruciale informatie uit die “operatie Othello” over te maken aan de onderzoekers en de onderzoeksrechter die gevat was in de zaak van de verdwenen meisjes die door Dutroux gevangen werden gehouden. Zie hierover Michel BOUFFIOUX en Marie-Jeanne VAN HEESWYCK, *La face cachée de l’enquête Dutroux et consorts*, Charleroi, Couleur livres, 2004, pp. 37-83.

¹⁹ Art. 44/1 WPA

²⁰ Christophe CALIMAN, « La gestion de l’information policière dans la loi du 7 décembre 1998 et les principes relatifs à la protection de la vie privée », *Revue de droit pénal et de criminologie*, avril 2000, p 415.

²² Deze gegevensbank wordt binnen het commissariaat-generaal van de federale politie beheerd (art. 44/4 WPA).

Gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Justitie en van Binnenlandse Zaken betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie (B.S. 18 juni 2002).

- het aankondigen van de organisatie van een betoging in Brussel gedurende een Europese top (concrete informatie van bestuurlijke politie);
- de informatie dat hooligans een voetbalwedstrijd willen verstoren door het aanvallen van de supporters van de tegenpartij (niet concrete informatie van bestuurlijke politie)”

In principe moet het gaan om objectieve en gecontroleerde informatie²³. Die informatie moet eveneens “in rechtstreeks verband staan met de bestaansreden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien..²⁴” In de praktijk is deze beperking weinig werkzaam. Het “doel” van het politiewerk betreft zowel het onderzoek en de voortzetting van de overtredingen maar ook elk aspect betreffende de handhaving van de openbare orde (bestuurlijke politie), hetgeen op erg brede wijze kan geïnterpreteerd worden. Het criterium van “het concrete belang” is betrekkelijk vaag en is in tegenspraak met het begrip “concreet gevaar”, gedefinieerd als “elke situatie waarin er voldoende vermoedens bestaan dat er een ernstige strafovertreiding werd gepleegd of kon gepleegd worden behalve indien er tegenstrijdige bewijzen zijn.”²⁵

I. 3.2. Wie profiteert van de twijfel?

Wat te doen in de gevallen waarin er twijfel bestaat over het concrete belang?

Men heeft de neiging te geloven dat de twijfel in het voordeel van de betrokken personen zou spelen en dat men niet zou overgaan tot het registreren van twijfelachtige gegevens. Nochtans zal, omdat het bijhouden van informatie voortaan onderhevig is aan zware sancties voor de politieagent²⁶, deze de neiging hebben om gegevens te verzamelen in geval van twijfel. Men kan zich dus afvragen of het niet registreren niet de uitzondering zal worden. De voorbeelden van zaken die niet in het ANG worden hernomen, zijn zeldzaam in de literatuur²⁷: Men haalt PV's aan betreffende vuur in een schoorsteen, familiegeschillen of het vandalisme in openbare telefooncellen²⁸.

Zoals hierboven uiteengezet, stelt de richtlijn die momenteel door de politieagenten wordt toegepast, dat een “niet-concrete” informatie, dat wil zeggen, niet gecontroleerd en niet definitief, een “concreet belang” kan hebben. Als de politieagent de enige rechter is van het “concreet belang”, belet niets dat een eenvoudig gerucht in de ANG wordt geregistreerd.

²³ Art. 44/1 WPA verwijst naar het art. 4 van de privacywet, wat bepaalt: “Persoonsgegevens dienen :

1° eerlijk en rechtmatig te worden verwerkt;

2° voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden te worden verkregen en niet verder te worden verwerkt op een wijze die (...) onverenigbaar is met die doeleinden. (...)

3° toereikend, terzake dienend en niet overmatig te zijn, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt;

4° nauwkeurig te zijn en, zo nodig, te worden bijgewerkt; alle redelijke maatregelen dienen te worden getroffen om de gegevens die, uitgaande van de doeleinden waarvoor zij worden verkregen of waarvoor zij verder worden verwerkt, onnauwkeurig of onvolledig zijn, uit te wissen of te verbeteren;

5° in een vorm die het mogelijk maakt de betrokkenen te identificeren, niet langer te worden bewaard dan voor de verwezenlijking van de doeleinden waarvoor zij worden verkregen of verder worden verwerkt, noodzakelijk is. (...)

²⁴ Art. 44/2 WPA.

²⁵ Aanbeveling R (87) 15 over het gebruik van persoonsgegevens op het terrein van de politie te herhalen aangenomen op 17 september 1987 door het Comité van de Ministers van de Raad van Europa Over de juridische waarde van dit instrument noteert Christian de Valkeneer « cette recommandation a acquis un caractère quasi conventionnel puisqu'il y est fait référence dans la Convention d'application de l'Accord de Schengen (article 115), dans la Convention sur le Système d'information Douanier (article 8) et dans la Convention Europol (article 14) » (Ch. de VALKENEER, Manuel de l'enquête pénale, Larcier, 2006, p 345, note 729).

²⁶ Art. 41/11 WPA: “Elke politieambtenaar die willens en wetens inlichtingen en gegevens die van belang zijn voor de uitoefening van de strafvordering of de handhaving van de openbare orde achterhoudt en nalaat door te zenden aan de algemene nationale gegevensbank overeenkomstig artikel 44/4, derde lid, wordt gestraft met gevangenisstraf van één maand tot zes maanden en een geldboete van zesentwintig tot vijfhonderd frank of met één van die straffen alleen.(...)”

²⁷ Art. 41/4 al. 4 WPA: “De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van zijn bevoegdheden, op eensluidend advies van het controleorgaan bedoeld in artikel 44/7, de categorieën van inlichtingen en gegevens die geen toezending vereisen” . Naar ons weten bestaat er nog geen openbare lijst van die elementen.

²⁸ G. BOURDOUX, A. LINERS, E. DE RAEDT, M. DE MESMAEKER, H. BERKMOES, La loi sur la fonction de police. Le Manuel de la fonction de police, Bruxelles, Politeia, 2005, p 300.

I. 3.3. Een toename van het aantal registraties in de ANG

Tabel: Aantal geregistreerde elementen in de ANG

Bron: Jaarlijks rapport van Comité P 2007-2008, p.36.²⁹

	2004	JULI 2006	DECEMBER 2006	DECEMBER 2007
CONCRETE FEITEN	8 826 227	> 10 000 000	11 086 899	12 359 250
NIET CONCRETE FEITEN	ONBESTAAND	INGEDEELD BIJ HIER-BOVEN VERMELD CIJFER	78 920	116 639
PERSONEN	1 425 904	1 764 052	1 644 435	1 745 208
WAGENS	1 486 155	1 749 471	1 824 630	2 077 099
PLAATSEN	5 887	24 091	15 877	22 124
ONDERZOEKEN	ONBESTAAND	GEEN CIJFERS	31 684	49 533
ORGANISATIES	ONBESTAAND	GEEN CIJFERS	11 547	18 886
NUMMERS	ONBESTAAND	GEEN CIJFERS	72 923	108 507
VOORWERPEN	11 641 688	14 590 426	15 390 444	17 464 197

Men kan zich enkel ongerust maken over de inflatie van deze cijfers. Indien we deze gegevens doortrekken, kan men bevestigen dat bijna één inwoner op zes in de gecentraliseerde gegevensbank van de geïntegreerde politie wordt opgenomen. De inflatie van het aantal “niet-concrete feiten” en “organisaties” is verontrustend wanneer men denkt aan de politieke fichage die uit de hand loopt en het gebrek aan controle van de betrouwbaarheid van de informatie³⁰. Van zijn kant verheugt het comité P zich over de stijging van de gegevens in de ANG: “omdat we tegelijk vaststellen dat er nu minder afzonderlijke databanken zijn en alles nu meer en meer beschikbaar is in één databank. Dit draagt bij tot een betere coördinatie en vergroot de controle mogelijkheden, maar ook de mogelijkheid tot correctie van gegevens (uniform beheer, toepassen ventilatieregels, klachten privacy, enz.)”³¹. Enkele paragrafen verder in zijn verslag, spreekt het Comité P zich tegen en stelt het vast dat er naast de ANG eveneens talrijke andere databases van allerlei soort bestaan (drugs, prostitutie, jeugdcriminaliteit, fotoalbums, huisarresten, bromfietsen, enz) zijn en „niemand een correct zicht op hun aantal laat staan op hun inhoud (heeft)”³². Volgens de Privacycommissie, hebben de politiediensten verklaard tussen 1995 en 2001 633 gegevens te hebben verwerkt. Tussen 2001 en 2005

²⁹ Voor dit laatste punt, zie verder.

³⁰ Over dit laatste punt, zie verder.

³¹ Comité P, jaarverslag 2007-2008, p 36. www.comitep.be

³² Ibid.

bedraagt dit cijfer slechts 89³³. Terwijl het grote aantal deze bestanden onrustwekkend³⁴ is, is het op zijn minst moeilijk, voor de burger, kennis te nemen van de volledige lijst³⁵.

I. 3.4. Bewaartijd? Onbepaald!

Deze vaststelling wordt versterkt door de afwezigheid van een bewaartermijn voorzien in een tekst. De aangiften ingediend bij de Privacycommissie vermelden een voorziene bewaartijd van 5 jaar voor de taken van de bestuurlijke politie en 10 jaar voor de gerechtelijke taken (zie bijlagen). Deze vermeldingen zijn indicatief. Momenteel worden de gegevens van ANG dus voor een onbepaalde duur bijgehouden, in afwachting van een wet die deze zaken zou ophelderen³⁶. Er is geen enkele duidelijke regel betreffende de afschaffing of het uitwissen van gegevens.

I. 3.5. Doorgeven van informatie aan andere Belgisch en buitenlandse overheden

De politieagenten kunnen informatie uit hun gegevensbanken doorgeven aan het gerecht, de politiediensten (Belgische- of buitenlandse), de inlichtingen- en veiligheidsdiensten, het comité P, het comité I, het Coördinatieorgaan voor de dreigingsanalyse (OCAD)³⁷, de algemene inspectie van de federale- en de lokale politie en aan de internationale organisaties van politiesamenwerking waarvoor de Belgische overheid verplichtingen heeft (met name Interpol en Europol). De politiedienst die de gegevens doorgeeft moet controleren of de ontvanger ze nodig heeft om zijn wettelijke taken uit te voeren en of de overdracht absoluut noodzakelijk is³⁸.

Voorts moeten de politieagenten de administratieve overheden (burgemeester...) op de hoogte brengen van "buitengewone gebeurtenissen betreffende de openbare orde", net zoals "de gewichtige feiten die de openbare rust, veiligheid of gezondheid in de gemeente kunnen verstoren"³⁹. Zij moeten eveneens de militaire autoriteiten informeren van "van alles wat de veiligheid van de strijdkrachten kan schaden" en van "alle propaganda waarbij de militairen tot tuchtelooheid worden aangezet" ⁴⁰.

³³ Liesbeth DE VIEGER, Nathalie VERSTUYFT, "Politieregisters en privacy", Gert VERMEULEN (ed.), Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen, Anvers / Appeldoorn, Maklu, 2007, p. 233.

³⁴ In het advies nr. 13/98 van 23 maart 1998 over het Voorontwerp van wet tot reorganisatie van de politiediensten, heeft de CBPL zich kritisch uitgesproken over de risico's ten gevolge van de proliferatie van gegevensverwerkingen en informatiestromen.

³⁵ Het ad hoc controleorgaan houdt een centraal register bij van de bijzondere gegevensbanken.

Enkel "de Minister van Binnenlandse Zaken of de persoon die hij delegeert, de Minister van Justitie of de persoon die hij delegeert, de bevoegde controle-autoriteiten, de gerechtelijke overheden, de overheden van bestuurlijke politie en de politiediensten" hebben toegang tot dat centraal register.. (art. 6 van het Koninklijk besluit houdende vaststelling van de voorwaarden betreffende de uitoefening van de opdrachten van het controleorgaan bedoeld in artikel 44/7 van de wet op het politieambt, B.S. 14 juni 2002). Over het openbaar register van de CBPL, zie verder.

³⁶ Een ontwerp van KB werd in 2008 door de Minister van Justitie opgesteld maar werd zo fel bekritiseerd zodat er uiteindelijk werd beslist een wetswijziging met een parlementair debat te organiseren. Die materies worden nu binnen een zogenaamde 'groep 44' besproken. Men verwacht een wetsontwerp tegen de zomer van 2010. .

³⁷ Het OCAD werd opgericht door de wet van 10 juli 2006.

³⁸ G. BOURDOUX, A. LINERS, E. DE RAEDT, M. DE MESMAEKER, H. BERKMOES, op. cit., 2005, p 295.

³⁹ Art. 5/2 WPA

⁴⁰ Art. 5/4 WPA

I. 4. Signalement: “kleine” vergissingen, ernstige gevolgen

In de jaren 90 moest een Belgische onderdane drie jaar wachten op een visum omdat zij geseind stond bij het Centraal Signalementenblad (CSB) ten gevolge van een fout afschrift van een verzoek van Interpol Washington en van een onvolledige verbetering van het foute bericht (het ging over een naamgenoot gecodeerd met een foutieve geboortedatum, die van het slachtoffer)⁴¹. In dezelfde periode werd een reserveofficier die gesignaleerd stond bij het CSB, op vraag van de militaire autoriteiten om hoofdzakelijk administratieve redenen uit zijn bed gelicht om 5u30 's ochtends na een controle van de fiches van het hotel waar hij verbleef. Hij werd vervolgens weggeleid naar de politiepost en opgesloten zonder dat iemand zich zorgen maakte over de echte redenen van het signalement bij het CSB⁴².

Deze voorbeelden tonen aan dat, in zoverre nodig, het respect voor het privéleven en een correcte behandeling van persoonlijke gegevens geen theoretische of abstracte aangelegenheid is. Een kleine onachtzaamheid hetzij bij codering, hetzij bij lezing van de gegevens van het signalement kunnen gevolgen hebben die het privéleven ver overstijgen en leiden tot schendingen van andere en meer zichtbare fundamentele rechten (hier de vrijheid van verkeer en vrijheid op zich).

Het Comité P meent dat “ambtenaren die aangelegenheden behandelen die betrekking hebben op de grondwettelijke en fundamentele rechten van de burgers, op een zeer uitdrukkelijke manier moeten gewezen worden op hun individuele verantwoordelijkheid en op het feit dat zij steeds grondig en nauwkeurig moeten handelen.” Ze stelt tevens dat het noodzakelijk is “dat bij elke stap in de procedure de tussenkomende ambtenaar individueel kan worden geïdentificeerd”, teneinde bij elke gebeurlijke fout de individuele verantwoordelijkheid, organisatorisch of structureel, te kunnen bepalen⁴³.

I.5. De “tricoche” of abusieve raadpleging van de databanken: anekdotisch?

Naast de bedreigingen van schending van het privéleven door praktijken zoals hierboven beschreven, is er een oud fenomeen: de abusieve raadpleging van databanken door politieagenten die “vergeten” dat ze hun bevoegdheden slechts mogen uitoefenen ten dienste van het algemeen belang en van hun wettelijke taken⁴⁴. De praktijk kan worden gemotiveerd door de loutere nieuwsgierigheid (nagaan of een beroemdheid “gekend is binnen de diensten”, om een voormalige collega die in de privé werkt te checken of om een journalist “een dienst te verlenen”⁴⁵). Van zodra de politieagent een tegenprestatie ontvangt spreken we van “tricoche” binnen het Franstalige politiejargon⁴⁶. Het is moeilijk om met precisie de grootte van het probleem te kennen, maar zelfs als ze beperkt is, is het feit dat gevoelige gegevens doorgegeven kunnen worden aan niet geautoriseerde personen heel onrustwekkend. Te meer dat, zoals reeds besproken, elke politieagent toegang heeft tot de ANG. De mogelijkheid om precies na te kunnen gaan wie welke

⁴¹ Bijzonder verslag 1999 van het Comité P, punt 6.1.1.

⁴² Ibid.

⁴³ Bijzonder verslag 1999 van het Comité P, punt 6.1.2.

⁴⁴ Dit fundamentele beginsel wordt bepaald door het artikel 12 van de Franse “Déclaration des droits de l’homme et du citoyen” van 1789,

⁴⁵ Na de dood van de bekende Vlaamse zangeres Yasmine in september 2009, hebben meer dan 900 leden van de politiediensten haar persoonsgegevens ingekeken De Morgen, 18/09/2009 <http://www.demorgen.be/dm/nl/989/Binnenland/article/detail/997727/2009/09/18/918-politiemensen-snuffelen-in-gegevens-Yasmine.dhtml>

⁴⁶ Assemblée nationale, in bovenvermeld Rapport d’information, pp. 143-149.

raadplegingen verricht, dringt zich op. Comité P pleit voor een “streng optreden” tegen leden van de politie die raadplegingen doen van persoonlijke gegevens buiten het kader van hun opdrachten van gerechtelijke en bestuurlijke politie of van andere administratieve taken⁴⁷. Zal het Comité worden gehoord?

Dit staaltje van bepaalde politiepraktijken toont ons inziens voldoende de nood aan van een democratische controle op de politiedatabanken. Rest ons nog kort te beschrijven hoe deze controle in de wettelijke bepalingen die op dit moment van kracht zijn in België is voorzien.

II. Welk inzagerecht heeft de burger met betrekking tot de politiedatabanken in België?

II.1. De basisprincipes met betrekking tot de bescherming van het privéleven en van de persoonsgegevens

Vooraleer het onderzoek van de politiedatabanken aan te snijden is het noodzakelijk even kort enkele basisprincipes in herinnering te brengen die algemeen van toepassing zijn op de databanken met persoonsgegevens. Dit zal toelaten om beter de draagwijdte te begrijpen van de afwijkingen waarvan de politie geniet.

De wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens⁴⁸ heeft aan deze materie een precies kader gegeven en heeft de Commissie voor de bescherming van de persoonlijke levenssfeer (verder genoemd de Commissie), in het levengeroepen. Dat is een instelling die formeel onder de vleugels van de Kamer van Volksvertegenwoordigers⁴⁹ is gebracht en die bevoegd is om advies en aanbevelingen te formuleren, en er moet voor zorgen dat de wet wordt nageleefd.

II. 1.1. De rechten van de geficheerde persoon tegenover de verantwoordelijke voor de verwerking van de gegevens

De basisgaranties die de burger ter beschikking staan tegen misbruik zijn samengevat de volgende:

- 1) verplichte aangifte van elke geautomatiseerde databank in het publieke domein aan de Commissie⁵⁰.
- 2) Verplichting van de ‘verantwoordelijke voor de verwerking’ om, vanaf de start van de inzameling, bepaalde informaties mee te delen aan de personen van wie hij de gegevens behandelt, met name: de

⁴⁷ Comité P, jaarverslag 2007-2008, p 40.

⁴⁸ Geconsolideerde versie beschikbaar op: http://www.privacycommission.be/nl/static/pdf/wetgeving/wet_privacy_08_12_1992.pdf. Zie ook het document van de CBPL : Bescherming van persoonsgegevens in België, 26 p.: http://www.privacycommission.be/nl/static/pdf/cbpl-documents/nota_privacy-algemeen.pdf. Zie ook de geannoteerde versie van de privacywet met heel veel referenties en samenvatting van de rechtspraak, een heel interessant werkinstrument van de CBPL : <http://www.privacycommission.be/nl/static/pdf/wetgeving/codex-nl-31-01-08-website.pdf>

⁴⁹ De CBPL bestaat uit acht vaste leden, onder wie ten minste één magistraat die het voorzitterschap waarneemt, en acht plaatsvervangende leden, onder wie ten minste één magistraat. De Ministerraad draagt lijsten voor die voor ieder te bekleden mandaat twee kandidaten bevatten, waarna de Kamer de leden benoemt. (art. 23 e.v. van de privacywet).

⁵⁰ De “papierbestanden” moeten dus niet aangegeven worden. Zie toch art. 19 van de privacywet : “Wanneer de Commissie voor de bescherming van de persoonlijke levenssfeer meent dat een niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin te worden opgenomen een mogelijke schending van de persoonlijke levenssfeer inhoudt, kan zij hetzij ambtshalve, hetzij op verzoek van een betrokkene de verantwoordelijke voor de verwerking opleggen haar mededeling te verstrekken van het geheel of een gedeelte van de inlichtingen opgesomd in artikel 17.”

doeleinden van de verwerking, de naam en het adres van de verantwoordelijke voor de verwerking, de mogelijkheid om zich te verzetten tegen direct marketing, het bestaan van een recht op toegang⁵¹.

3) Het onvoorwaardelijk recht, voor iedere persoon die zijn identiteit aantoont, om van de verantwoordelijke voor de verwerking te bekomen, ten laatste binnen de 45 dagen na zijn gedateerd en ondertekend verzoek:

- a) bevestiging dat de hem betreffende gegevens al dan niet verwerkt zijn, evenals de informatie die minstens betrekking heeft op de doeleinden van de verwerking, de categorieën waarvoor de gegevens verwerkt zijn en de categorieën ontvangers aan wie de gegevens worden verstrekt;
- b) verstrekking in begrijpelijke vorm van de gegevens zelf die worden verwerkt, alsmede alle beschikbare informatie over de oorsprong van de gegevens;
- c) mededeling van de logica die aan een geautomatiseerde verwerking van hem betreffende gegevens ten grondslag ligt, in geval van geautomatiseerde besluitvorming;
- d) kennisgeving van de mogelijkheid om de in de artikelen 12 en 14 bedoelde beroepen in te stellen en eventueel inzage te nemen van het openbaar register bij de Commissie⁵².

4) het recht om op eenvoudige gedateerde en schriftelijk vraag gericht aan de verantwoordelijke van de verwerking:

- a) kosteloos de verbetering te bekomen van alle onjuiste persoonsgegevens⁵³;
- b) zich 'wegens zwaarwegende en gerechtvaardigde redenen die verband houden met zijn bijzondere situatie'⁵⁴ te verzetten dat hem betreffende gegevens worden verwerkt⁵⁵;
- c) kosteloos de verwijdering van of het verbod op de aanwending van alle hem betreffende persoonsgegevens te bekomen die gelet op het doel van de verwerking, onvolledig of niet ter zake dienend zijn, of waarvan de registratie, de mededeling of de bewaring verboden zijn, of die na verloop van de toegestane duur zijn bewaard.

5) de verplichting in hoofde van de verantwoordelijke voor de verwerking, om binnen de maand na het verzoek, de verbeteringen of verwijderingen van gegevens mee te delen, of het gevolg mee te delen dat aan het verzoek werd gegeven, zowel aan de betrokken persoon als aan de personen aan wie de onjuiste, onvolledige of niet ter zake dienende gegevens werden meegedeeld, 'voor zover hij nog kennis heeft van de bestemmingen van de mededeling en de kennisgeving aan deze bestemmingen niet onmogelijk blijkt of onevenredig veel moeite kost'⁵⁶.

II. 1.2. Specifiek juridisch beroep en schadeloosstelling door de verantwoordelijke van de databank

De persoon van wie de hierboven beschreven rechten niet gerespecteerd werden kan een vordering instellen bij de Voorzitter van de rechtbank van eerste aanleg, zoals in kort geding⁵⁷. Deze vordering is slechts ontvankelijk wanneer het verzoek tot toegang of rechtzetting verworpen is of als er binnen de voorziene

⁵¹ Art. 9 van de privacywet.

⁵² Art. 10 § 1 van de privacywet

⁵³ Art. 12 §1 lid 1 van de privacywet

⁵⁴ Art 12 §1 lid. 2 van de privacywet

⁵⁵ Dit is niet van toepassing : - "wanneer de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of voor de uitvoering van maatregelen die aan het sluiten van die overeenkomst voorafgaan en die op verzoek van de betrokkene zijn genomen;" en "wanneer de verwerking noodzakelijk is om een verplichting na te komen waaraan de verantwoordelijke voor de verwerking is onderworpen door of krachtens een wet, een decreet of een ordonnantie;" (art. 12 §1 lid 2 juncto art. 5 b) en c) van de privacywet).

⁵⁶ Art. 12 § 3 van de privacywet .

⁵⁷ "zoals in kort geding" art. 14 §1 van de privacywet

termijn geen gevolg is aan verleend⁵⁸. Wanneer er 'dringende redenen' de vrees doen rijzen dat de verantwoordelijke voor de databank bewijsmateriaal zou kunnen verhelen of doen verdwijnen, kan de rechter met een eenzijdig verzoekschrift gevat worden opdat hij elke maatregel zou bevelen ter voorkoming van die verhelings of verdwijning. Tijdens de ganse procedure is de verantwoordelijke voor de verwerking verplicht duidelijk aan te geven, tijdens elke mededeling van het desbetreffende gegeven, dat dat gegeven betwist is⁵⁹.

Indien een persoon 'een schade lijdt doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens deze wet bepaalde voorschriften', moet de verantwoordelijke voor de verwerking de betrokkene schadeloos stellen, behalve wanneer hij bewijst dat het feit dat de schade heeft veroorzaakt hem niet kan worden toegerekend⁶⁰.

II. 1.3. Enkele garanties die niet van toepassing zijn op de databanken van de politie

De openbare overheden die databanken beheren met het oog op de uitoefening van hun opdrachten van gerechtelijke politie, de politiediensten en andere autoriteiten die gegevens behandelen voor doeleinden van bestuurlijke politie⁶¹, zijn vrijgesteld van de hogerbeschreven verplichtingen, met uitzondering van de aangifte ervan aan de Commissie⁶². Dit betekent dat de burger niet het recht heeft verwittigd te worden dat zijn persoonsgegevens gebruikt worden door de politie. Hij heeft evenmin het recht om bij de verantwoordelijke voor de verwerking informatie te bekomen over de databanken, en nog minder om de rechtzetting of verwijdering van de gegevens te verzoeken. Noteren we nochtans dat voor het overige, de oprichting en de behandeling van de politiedatabanken, moet gebeuren conform alle andere bepalingen van de wet verwerking persoonsgegevens, en de politie deze bepalingen bijgevolg moet respecteren⁶³.

II.2 het recht om het bestaan te kennen van een politiebestand.

Het is theoretisch mogelijk om het bestaan van elk politiebestand te kennen⁶⁴. De politie is immers verplicht om van elke "volledig of gedeeltelijk geautomatiseerde verwerking van gegevens" ⁶⁵ een aangifte te doen bij de CBPL. De aangifte moet verplicht een aantal elementen bevatten, het doel, de volledige gegevens van 'de verantwoordelijke voor de verwerking', de duur van de bewaring van de gegevens en de garanties die een eventuele transmissie naar derden. Het is niet onnuttig op te merken dat bij afwezigheid van een dergelijke aangifte, strafsancities kunnen volgen⁶⁶. Men vindt bijgevolg een aantal politiebestanden terug op een publiek register van de CBPL, terug te vinden op het webadres:

<https://www.privacycommission.be/elg/searchPR.htm?eraseResults=true&siteLanguage=nl>

⁵⁸ Art. 14 §5 van de privacywet

⁵⁹ Art. 15 van de privacywet

⁶⁰ Art. 15 bis van de privacywet

⁶¹ Art. 3 §5 van de privacywet

⁶² Krachtens art. 3 §5 van de privacywet zijn artikels 9, 10, § 1, en 12 niet van toepassing.

⁶³ Zie Art. 44/2 WPA: "Het inwinnen, de verwerking en het toezenden van de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, gebeurt overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Deze inlichtingen en gegevens moeten in rechtstreeks verband staan met de bestaansreden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien".

⁶⁴ Zie hoger. Wanneer een particulier meent dat een niet-geautomatiseerde databank een inbreuk op zijn privéleven uitmaakt, kan hij de CBPL verzoeken om de politiedienst te dwingen aangifte van deze databank te doen. (art. 19 van de privacywet).

⁶⁵ Art. 17 van de privacywet

⁶⁶ Met geldboete van honderd euro tot honderdduizend euro (art. 39, 7° van de privacywet).

Nochtans is in de praktijk het terugvinden van deze informatie niet makkelijk omdat de methoden die gebruikt worden om deze verklaring af te leggen niet eenvormig zijn en omdat de ambtenaren die deze verklaringen afleggen vaak karig zijn met de informatie. Een poging doen om een volledige lijst te maken van alle politiebestanden is heel moeilijk, vooral ook omdat het Comité P vermoedt dat vele politiezones gebruik maken van de politiebestanden, zonder hierover een voorafgaande verklaring af te leggen bij het CBPL⁶⁷. Ten slotte dient opgemerkt te worden dat de inlichtingsdiensten dit probleem niet hebben: zij ontsnappen volledig aan de verplichting om dergelijke verklaring af te leggen⁶⁸.

II.3 geen recht om te weten of men al dan niet voorkomt in een politiebestand

II.3.1 indirecte toegang via de De Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)

In België is een directe toegang tot de gegevens waarover de politie beschikt niet toegelaten. Men moet verplicht via de CBPL gaan, die deze controle kan uitvoeren, op vraag van een geïdентificeerde persoon⁶⁹. Om dit te doen, moet men een gedateerde en getekende aanvraag sturen aan de CBPL. Op straffe van onontvankelijkheid, dient deze aanvraag de volgende gegevens te bevatten: naam, voornaam, geboortedatum, nationaliteit van de betrokkene, kopie van zijn identiteitsdocument. Men dient eveneens aan te geven om welke bevoegde autoriteit of dienst het gaat en 'alle relevante elementen betreffende de betwiste gegevens zoals de aard ervan, de omstandigheden of de aanleiding van de kennisneming ervan, alsook de eventueel gewenste verbeteringen⁷⁰', te vermelden.

De CBPL kan eisen dat de politie de gevraagde wijzigingen aanbrengt, of verkeerde gegevens weglaat⁷¹. Ze heeft in principe niet het recht de betrokkene te informeren welke actie er juist werd ondernomen. De betrokkene zal evenmin enige andere informatie verkrijgen behalve een bericht dat 'de nodige verificaties verricht werden.⁷²' De betrokkene kan bijgevolg niet weten of hij werkelijk in het bestand stond en nog minder welke informatie er over hem in het bestand te vinden was. Het is eveneens onmogelijk te weten of de gegevens verbeterd of weggehaald werden. Men dient één jaar te wachten vooraleer men een nieuwe aanvraag kan indienen betreffende dezelfde gegevens, behalve wanneer de CBPL een uitzondering toestaat na een gemotiveerde aanvraag hiertoe⁷³.

Rekening houdende met deze beperkingen, is het niet verbazingwekkend dat deze procedure zo weinig gebruikt wordt. In 2008 werd de Commissie 159 keer gevat⁷⁴. Dit cijfer is al een sterke stijging ten aanzien van 2007⁷⁵. Is deze procedure hierdoor totaal nutteloos? Toch niet, als men de CBPL moet geloven. Die stelt dat bijna drie vierde van de aanvragen, afgesloten in 2008, hebben geleid tot een gehele of gedeeltelijke verwijdering van de aanwezige gegevens, zoals de tabel hieronder aantoont.

⁶⁷ Comité P, jaarverslag 2007-2008, www.comitep.be

⁶⁸ Art. 3 § 4 van de privacywet.

⁶⁹ De procedure wordt door artikel 13 van de privacywet bepaald. Zie ook artikel 36 e.v. van het Koninklijk Besluit van 13 februari 2001 ter uitvoering van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (B.S. 13 maart 2001).

⁷⁰ Art. 37 van het KB van 13 februari 2001

⁷¹ De Commissie kan politiediensten "gegevens doen verbeteren of verwijderen, of gegevens doen invoeren. Zij kan de mededeling van de gegevens te verbieden." (43 van het KB van 13 februari 2001). Tegenover inlichtingendiensten "beveelt de Commissie de maatregelen aan die ze noodzakelijk acht" maar kan ze niets afdwingen.

⁷² Art. 46 van het KB van 13 februari 2001. Ingeval van identiteitsgegevens "verstrekt de Commissie, na advies van de betrokken dienst, aan de betrokken persoon alle andere inlichtingen die zij relevant acht."

⁷³ Art. 40 van het KB van 13 februari 2001.

⁷⁴ CBPL, Jaarverslag 2008, p. 56.

⁷⁵ In 2007: 87 aanvragen ; in 2006: 91 aanvragen (CBPL, Jaarverslag 2007, p. 60.)

Analyse "dossiers 13" afgesloten in 2008 (13-2007 en 13-2008)

	Aantal	%
Gevolg		
Gehele schrapping	33	56,90
Gedeeltelijke schrapping	10	17,24
Behoud gegevens	10	17,24
Niet geregistreerd	5	8,62

Bron: CBPL, Jaarverslag 2008, p. 71

Ondanks de beperkingen van deze procedure, kunnen we mensen alleen maar aanmoedigen die een potentieel bestand willen aanvechten om gebruik te maken van hun recht hiertoe. Een modelaanvraag is terug te vinden op de website van het CBPL en is ook als bijlage toegevoegd aan huidige bijdrage. Volgens sommigen is de uitzondering die actueel in België gemaakt wordt op de toegang tot politiebestanden en het recht op rectificatie ervan te ruim en zou de wet moeten gewijzigd worden⁷⁶.

II.3.2 het ad hoc controle-orgaan van de geïntegreerde politie

De wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst heeft een intern controleorgaan ingesteld bij de politie, specifiek belast met de ANG en de correcte toepassing van de politiepraktijken inzake informatie⁷⁷. In de praktijk is het dus vaak een gesprekspartner voor de CBPL wanneer zij controles uitvoert. Dit orgaan is samengesteld uit een lid van de lokale politie, een lid van de federale politie en een expert. Het orgaan wordt voorgezeten door een federale magistraat aangeduid door de minister van justitie en de minister van binnenlandse zaken, op voorstel van de federale procureur. De magistraat handelt voor de duur van zijn aanwijzing "onafhankelijk ten aanzien van het federaal parket"⁷⁸. Dit orgaan heeft "op de politieambtenaren niet meer dan een controle met betrekking tot de manier waarop zij deelnemen aan het globale concept van informatiebeheer : hebben zij geen informatie achtergehouden,, heeft men geen aparte gegevensbanken gecreëerd zonder toelating,, heeft men geen kennis genomen van gegevens die men niet hoefde te kennen voor de uitoefening van de functie (" need to know ") . enz."⁷⁹. Het nut voor de burger van dit orgaan is quasi onbestaand, omdat geen enkele wettekst toestaat dat de burger er zich toe wendt⁸⁰. Evenmin is er een wettekst die het verbiedt; waarom zou men dus niet proberen om ook bij dit controleorgaan te bekomen dat bepaalde verkeerde informatie verbeterd wordt? Het valt af te wachten of dit controleorgaan gevoelig is voor de klachten van burgers met betrekking tot hun privé-leven. Uit het laatste jaarrapport van het Comité P blijkt dat het controleorgaan eigenlijk vooral hoopt dat er op een nog efficiëntere manier gegevens kunnen worden verzameld en dat bij uitstek betreurd wordt dat vingerafdrukken, foto's en volledige

⁷⁶ Liesbeth DE VIEGER, Nathalie VERSTUYFT, "Politiregisters en privacy", Gert VERMEULEN (ed.), Privacy en strafrecht. Nieuwe en grensoverschrijdende verkenningen, Antwerpen/ Appeldoorn, Maklu, 2007, p. 227.

⁷⁷ Zie art. 44/7 WPA en KB van 30 mei 2002 houdende vaststelling van de voorwaarden betreffende de uitoefening van de opdrachten van het controleorgaan bedoeld in artikel 44/7 van de wet op het politieambt (B.S. 14 juni 2002).

⁷⁸ Art. 44/7 lid 5 WPA.

⁷⁹ Verslag aan de Koning bij het bovenvermeld KB van 30 mei 2002.

⁸⁰ Zie bovenvermeld KB van 30 mei 2002 en huishoudelijk reglement van 17 juni 2003 (B.S. 9 september 2003).

fysieke beschrijvingen van aangehouden personen niet systematisch in het ANG voorkomen⁸¹. De missies van dit orgaan komen gedeeltelijk overeen met die van de Commissie ter bescherming van het privéleven en die van het Comité P. Het argument dat er een risico op cumul van bevoegdheden bestaat tussen het intern controleorgaan van de politie, de CBPL en het Comité P was in 2002 ingeroepen door de regering om de bevoegdheden van het intern controleorgaan te kunnen beperken. Volgens de Raad van State is deze beperking van bevoegdheden onwettig: "Aangezien de wetgever het dienstig heeft geacht in verschillende vormen van controle te voorzien, staat het niet aan de Koning om die vormen van controle te beperken ten einde overlappingen te voorkomen."⁸²

Zoals we gezien hebben, heeft de burger geen werkelijk recht om te weten welke politiebestanden er over hem bestaan. Hij moet zich tevreden stellen met een indirect recht van toegang en wordt geacht een blind vertrouwen te hebben in de CBPL. Ook al heeft deze een injunctierecht om aan de politiedienst te bevelen bepaalde gegevens te verbeteren of weg te laten, toch kan men zich de vraag stellen of dit systeem voldoende is en de fundamentele mensenrechten respecteert.

III. Conformiteit van de Belgische praktijk met het Europees Verdrag voor de Rechten van de Mens

Het is interessant om het hierboven beschreven controlemechanisme te confronteren met enkele belangrijke arresten van het Europees Hof voor de Rechten van de Mens met betrekking tot het recht op eerbiediging van het privéleven en het recht op een effectief rechtsmiddel.

III.1. Het recht op Privacy

Het artikel 8 van het EVRM ("Recht op eerbiediging van privéleven, familie- en gezinsleven") luidt als volgt:

- "1. Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

⁸¹ "Zij controleerden, op basis van de lijsten van aangehouden personen (cf. register der aangehouden personen), voor wie de gerechtelijke "driedelige identificatie" (foto, vingerafdrukken en individuele beschrijving) correct werd uitgevoerd. Bij een controle van de overgemaakte gegevens van 12.383 personen in de ANG bleek er (1) voor 68 % geen foto aanwezig te zijn, (2) bij 73 % de individuele beschrijving te ontbreken en (3) bij 60 % geen vingerafdrukken aanwezig te zijn." Het Comité P beschouwt dit als "een zeer groot gevaar" dat verhindert om mogelijke daders te identificeren. Comité P, Jaarverslag 2007-2008, p 38. www.comitep.be

⁸² Advies van de Raad van State nr. 31.932/2 in bijlage van het KB van 30 mei 2002 (B.S. 14 juni 2002). Over de controle van het Comité P, zie de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse.

III. 1.1. Definitie van Privacy in het kader van dataverwerking

Sommige staten verdedigen de stelling dat publieke activiteiten (openbare vergaderingen, betogingen, petitie op het internet, publiceren van politieke brochures...) het voorwerp mogen uitmaken van een grenzeloze controle en fichering omdat deze zaken niet zouden vallen onder de privacy van de burger.

Het Hof heeft die enge interpretatie van priv  sfeer verworpen. Verwijzend naar het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens van 28 januari 1981, meent het Hof dat elke informatie over een ge  dentificeerd of identificeerbaar⁸³ fysiek persoon die het voorwerp uitmaakt van geautomatiseerde gegevensverwerking, een schending kan uitmaken van het recht op priv  leven.

Het Hof bevestigt daarnaast dat gegevens die openbaar zijn tot het priv   leven kunnen behoren wanneer ze systematisch, opgeslagen worden in door de overheid georganiseerde databanken⁸⁴. Het Hof stelt verder dat dit zelfs nog meer geldt wanneer de gegevens stammen uit een ver verleden van een persoon.

III.1.2. Bestaan van een inmenging

Zowel het opslaan van gegevens betreffende het priv  leven van een individu door de overheid, als het gebruik van deze gegevens, als de weigering om deze gegevens te verbeteren of te weerleggen, maken een inmenging uit in het recht op een priv  leven, gevrijwaard door art. 8, lid 1 EVRM⁸⁵. Aangezien men in België niet het recht heeft om de gegevens die de overheid van de burger bijhoudt te betwisten, is er sprake van onmogelijkheid tot verbetering of weerlegging.

Wanneer men zich tot de CBPL wendt, komt men nooit te weten of er gegevens worden verbeterd of niet, behoudens wanneer het om een identiteitsfout gaat. De weigering om de betrokkene te informeren over welke informatie over hem of haar door de politie in geheime databanken wordt bijgehouden, maakt volgens het Hof een inmenging uit in het priv  -leven⁸⁶. Er bestaat dus weinig twijfel over dat de politiedatabank, zoals de gecentraliseerde ANG-databank, een inmenging uitmaakt van het recht op privacy.

Zo'n inmenging is slechts toelaatbaar wanneer ze voorzien is bij wet, een legitiem doel nastreeft overeenkomstig paragraaf twee van art. 8 EVRM en indien de inmenging noodzakelijk is in een democratische maatschappij.

Laten we kort ieder van deze elementen onderzoeken.

⁸³ Europees Hof voor de Rechten van de Mens (hierna "EHRM"), *Amann c. Suisse* [GC], du 16 f  vrier 2000, beschikbaar, zoals alle geciteerde arresten, op <http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-fr>

⁸⁴ EHRM, *Rotaru t. Roemeni  * van 4 mei 2000,    43. Zie toch de afwijkende mening van de rechter Bonello: « Le militantisme public au sein de partis politiques publics n'a (...) rien    voir avec le principe qui commande d'  lever la protection de la vie priv  e au rang de droit fondamental. » (   6). Maar het Hof heeft zijn rechtspraak bevestigd in de zaak *Segerstedt-Wiberg en anderen t. Zweden* van 6 juni 2006,    72.

⁸⁵ EHRM, arrest *Leander t. Zweden* van 26 maart, 1987, reeks A no 116, eerder geciteerd, p. 22,    48, *Kopp t. Zwitserland* van 25 maart 1998, Recueil 1998-II, p. 540,    53, en *Amann* eerder geciteerd,       69 en 80, *Rotaru t. Roemeni  *, 4 mei 2000, nr. 28341/95,    46.).

⁸⁶ EHRM *Segerstedt-Wiberg en anderen t. Zweden* van 6 juni 2006,    99.

III. 1.3. Inmenging bij wet voorzien

De woorden « bij wet voorzien » verplichten niet enkel een wettelijke basis voor inbreukmakende maatregelen; de wetgeving moet bovendien toegankelijk zijn en voorzienbaar voor de rechtsonderhorige⁸⁷. Een rechtsregel is « voorzienbaar » wanneer ze voldoende precies is opgesteld, zodat het mogelijk wordt zijn gedrag aan de regel aan te passen. Deze vereiste biedt bescherming tegen willekeurige inmenging van het openbaar gezag in het privé leven. Het Hof onderlijnt dat het gevaar van een willekeurige inmenging sterker is wanneer de uitvoerende macht in het geheim handelt. Om individuen genoeg bescherming te geven tegen willekeur is het bovendien noodzakelijk dat de modaliteiten en het bereik van de maatregel precies gedefinieerd worden⁸⁸.

In België slaat men een aanzienlijke hoeveelheid persoonsgegevens op, ondermeer in de ANG, met als argument dat hierdoor een “concreet belang” gediend wordt. Het valt te betwijfelen dat zo’n vaag criterium de voorwaarde van voorzienbaarheid respecteert, des te meer omdat het momenteel is toegestaan dat de gegevens onbeperkt worden bijgehouden. Het KB dat wordt verondersteld de modaliteiten betreffende gegevensbeheer te reglementeren (onder meer hoe lang de gegevens moeten worden bijgehouden) laat immers reeds 12 jaar op zich wachten.

In de reeds vernoemde zaak Rotaru, is het onder andere het ontbreken van een termijn vastgesteld door de wet, dat het Hof deed besluiten dat de inmenging niet werd voorzien door de wet⁸⁹.

Men dient tevens vast te stellen dat gevoelige gegevens zoals ethnische origine, politieke mening, syndicaal lidmaatschap... op de dag van vandaag vrolijk worden verzameld en bijgehouden. Dit blijkt duidelijk uit aangiften van de politiedatabanken ingediend in het openbaar register van de CBPL.

Bijvoorbeeld bij de aangifte ANG bestuurspolitie, vinden we in de rubriek « Categorieën van gegevens die verwerkt worden » niet alleen de traditionele identificatiegegevens (naam, adres, tel,...), elektronische gegevens (IP adressen, Cookies,...) en biometrische gegevens, maar ook « beroep », « lidmaatschappen » zonder verdere precisie (mutualiteit, vakbond, ??), « raciale of ethnische gegevens », « Politieke opvattingen » en « Filosofische of religieuze overtuigingen ». (zie bijlage)

De wet voorziet wel degelijk dat de politie gevoelige gegevens mag verwerken, maar deze verwerking dient te gebeuren « op de wijze bepaald door de Koning, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer »⁹⁰. Nochtans is er, zoals iedereen weet, sinds de wet van 1998 ter oprichting van de ANG, geen enkel Koninklijk Besluit verschenen om de modaliteiten vast te stellen. Dit stelt duidelijk een probleem met betrekking tot de garanties tegen misbruik die het Hof vereist. Een geheim controlesysteem bedoeld de nationale veiligheid te beschermen houdt het risico in om de democratie te ondergraven en te vernietigen onder het mom van de bescherming van deze democratie⁹¹.

⁸⁷ Zie o. a. het bovenvermeld arrest Amann, § 50.

⁸⁸ EHRM, Malone t. Verenigd Koninkrijk van 2 augustus 1984, § 67, arrest Amann eerder geciteerd, § 56 en Rotaru eerder geciteerd, § 55.

⁸⁹ Rotaru eerder geciteerd, § 37.

⁹⁰ Art 44/1 lid 2 WPA.

⁹¹ Arrest Klass en anderen t. Duitsland van 6 september 1978, 23-24, §§ 49-50.

III. 1.4. Inmenging met een legitiem doel

Het opstellen van een politiedatabank streeft een legitiem doel na zoals voorzien in het art 8 lid 2⁹². Hierover bestaat weinig twijfel.

In een interessante zaak oordeelde het Hof van Straatsburg op 6 juni 2006 dat het bijhouden, door de Zweedse inlichtingendienst, van informatie betreffende de deelname van een welbepaalde persoon aan een politieke vergadering in Warschau in 1976 « rekening houdend met de aard en de ouderdom van de informatie (...) niet gemotiveerd werd door een legitieme en voldoende ernstige doelstelling ten aanzien van de bescherming van de nationale veiligheid. »⁹³, Het Hof voegt eraan toe: « De même, la conservation de la majeure partie des informations divulguées au cinquième requérant ne peut guère passer pour répondre à des intérêts de sécurité nationale véritablement pertinents pour l'Etat défendeur. La conservation des renseignements selon lesquels l'intéressé aurait, en 1969, préconisé d'opposer une résistance violente aux contrôles de police durant des manifestations se fonde sur des motifs qui, malgré leur caractère pertinent, ne sauraient passer pour suffisants trente ans plus tard »⁹⁴. Men kan hieruit afleiden dat er geen sprake kan zijn van een legitiem doel, indien er geen redelijke band is tussen het bijhouden van de gegevens en de verwezenlijking van dat doel.

Thomas Hammarberg, mensenrechtencommissaris van de Raad van Europa, definieert op de volgende manier de voorwaarden die dienen vervuld te worden om te beantwoorden aan het beginsel van legitimiteit:

- « • men dient zo precies mogelijk te zijn; het volstaat niet te wijzen op het feit dat het behandelen van gegevens behoort tot het werkkader van de politie zelfs niet van een specifieke taak van de politie (strafrechtelijk onderzoek en vervolging, reactie op een onmiddellijke dreiging of nog preventie);
- de persoonsgegevens verzameld voor een welbepaalde politieke noodzaak (bijvoorbeeld het afwenden van een dreiging) mogen niet gebruikt worden voor anderen doelen (bijvoorbeeld het onderzoeken van een misdrijf) tenzij deze gegevens ook voor deze tweede doelstelling op een onafhankelijke wijze hadden kunnen verzameld worden;
- de persoonsgegevens mogen nooit verzameld worden door de politie of andere diensten die de wet moeten toepassen « voor het geval dat »⁹⁵.

Nogmaals, men kan zich afvragen of het weinig precieze karakter van de term « concreet belang » voor het geheel van de opdrachten van de politie deze finaliteitsvoorwaarde vervult.

⁹² Zie toch de opinie van de rechter Wildhaber, goedgekeurd door Makarczyk, Türmen, Costa, Tulkens, Casadevall en Weber na het arrest Rotaru: « Quant à la question du but légitime, la Cour admet d'ordinaire sans difficulté la légitimité de l'objectif défini par le Gouvernement sous réserve qu'il relève de l'une des catégories visées au paragraphe 2 des articles 8 à 11. Toutefois, pour la sécurité nationale comme pour d'autres buts, j'estime qu'il doit exister au moins un lien raisonnable et réel entre les mesures portant atteinte à la vie privée et l'objectif invoqué pour que celui-ci puisse être considéré comme légitime. A mon sens, expliquer que la conservation, pour ainsi dire sans discernement, d'informations relatives à la vie privée d'individus correspond à un souci légitime de sécurité nationale pose manifestement un problème. »

⁹³ EHRM Segerstedt-Wiberg en anderen t. Zweden van 6 juni 2006, § 90.

⁹⁴ Ibid.

⁹⁵ Commissaris voor de mensenrechten van de Raad van Europa, Lutte contre le terrorisme et protection du droit au respect de la vie privée, CommDH/IssuePaper(2008)3, p 9 (vrije vertaling uit het Frans).

III. 1.5. Noodzakelijk in een democratische maatschappij

Opdat een inmenging toelaatbaar is de zin van het artikel 8, moet deze inmenging voldoen aan de hierboven beschreven voorwaarden, maar de inmenging moet ook « noodzakelijk zijn in een democratische samenleving ».

Enkele Straatsburgse rechters verwoordden het zo:

« Les États ne disposent pas d’une latitude illimitée pour assujettir les individus à des mesures de surveillance secrète ou à un système de fichiers secrets. L’intérêt d’un Etat à préserver sa sécurité nationale doit être mis en balance avec la gravité de l’atteinte au droit d’un requérant au respect de sa vie privée.»⁹⁶

Volgens Thomas Hammarberg helt de weegschaal in de richting van het respect voor het privéleven voor wat gevoelige gegevens betreft. Hij bevestigt dat: « het verzamelen van persoonsgegevens met als enige argument het behoren tot de ene of de andere raciale origine, een welbepaalde religieuze overtuiging, seksuele geaardheid of omwille van een welbepaalde politieke mening, lidmaatschap van een organisatie of beweging die niet verboden is bij wet, zou verboden moeten zijn » tenzij « deze informatie absoluut noodzakelijk is voor de noden van een welbepaald onderzoek. »⁹⁷

In de reeds genoemde Zweedse zaak, werd geoordeeld dat lidmaatschap van een politieke partij « die gebruik van geweld en inbreuken van de wet voor het veranderen van de sociale orde als doel heeft » niet als voldoende reden wordt beschouwd om gegevens bij te houden. Het Hof besluit: « (...) le Gouvernement n’indique aucune circonstance spécifique qui montrerait que les dispositions litigieuses du programme ont trouvé leur expression dans les actes et déclarations des dirigeants ou membres du parti et ont constitué une menace réelle, ou même simplement potentielle, pour la sécurité nationale lorsque les informations ont été divulguées en 1999, soit près de trente ans après la création du parti. Dès lors, les motifs ayant justifié la conservation des informations relatives aux troisième et quatrième requérants, bien que pertinents, ne sauraient être considérés comme suffisants aux fins du critère de nécessité à appliquer sous l’angle de l’article 8 § 2 de la Convention. En conséquence, la conservation des informations communiquées aux requérants concernés en 1999 s’analyse en une ingérence disproportionnée dans l’exercice par les intéressés de leur droit au respect de leur vie privée»⁹⁸.

Opnieuw stelt zich het probleem van de duur van het bijhouden van de gegevens en van het ontbreken van de modaliteiten betreffende de verwerking en de verzameling van de gegevens voor de verschillende databanken van de politie. In de huidige stand van zaken zijn een groot deel van de gegevens die momenteel worden bijgehouden ‘uit voorzorg’ in realiteit niet nodig in een democratisch systeem dat zichzelf respecteert.

⁹⁶ Mening van de rechter Wildhaber, in de zaak Rotaru eerder geciteerd. Hij verwijst naar de volgende zaken: arrest Leander t. Zweden van 26 maart 1987, reeks A no 116, p. 25, § 60; zie ook l’arrest Klass en anderen t. Duitsland van 6 september 1978, reeks A no 28, pp. 21 en 23, §§ 42 en 49 en, mutatis mutandis, het arrest Chahal t. Verenigd Koninkrijk van 15 november 1996, Recueil 1996-V, pp. 1866 1867, § 131, en het arrest Tinnelly & Sons Ltd en anderen en McElduff en anderen t. Verenigd Koninkrijk van 10 juli 1998, Recueil 1998-IV, pp. 1662 1663, § 77.

⁹⁷ Commissaris voor de mensenrechten van de Raad van Europa CommDH/IssuePaper(2008)3, p 10 (verwijzend naar het principe 2.4 van de aanbeveling nr. R(87)15)

⁹⁸ EHRM Segerstedt-Wiberg en anderen t. Zweden van 6 juni 2006, § 91.

III. 2. Het recht op een daadwerkelijk rechtsmiddel (artikel 13)

Het artikel 13 van het EVRM stelt het volgende:

« Een ieder wiens rechten en vrijheden die in dit verdrag zijn vermeld, zijn geschonden, heeft recht op een daadwerkelijk rechtsmiddel voor een nationale instantie, ook indien deze schending is begaan door personen in de uitoefening van hun ambtelijke functie. »

Indien een individu klaagt over privacyschendende dataverwerking door de politie, zou hij moeten kunnen genieten van een daadwerkelijk rechtsmiddel om zijn recht op privéleven te doen respecteren. Het is niet noodzakelijk te bewijzen dat het artikel 8 werd geschonden om recht te hebben op het daadwerkelijk rechtsmiddel. Het volstaat een bezwaar te hebben dat men als « verdedigbaar » kan beschouwen⁹⁹. In tegenstelling met de voorwaarde vooropgesteld door het artikel 6 van het EVRM, legt het artikel 13 niet op dat het moet gaan om een « onafhankelijk en onpartijdig gerecht » doch enkel een « bevoegde nationale instantie » die de mogelijkheid heeft om kennis te nemen van de inhoud van de klacht en eventueel het gepaste herstel kan aanbieden¹⁰⁰. Volgens het Hof moeten de beslissingen van deze instantie bindend zijn ten aanzien van de politie¹⁰¹. De beslissingen van de CBPL zijn bindend ten aanzien van de politie, aangezien zij de opdracht kan geven om bepaalde gegevens te wissen of te verbeteren of kan verplichten om afwijkende gegevens in te voeren. Zij kan ook verbieden dat bepaalde gegevens worden medegedeeld.¹⁰²

Een meer pertinente vraag die men zich dient te stellen is of er wel sprake kan zijn van een daadwerkelijk rechtsmiddel indien dit rechtsmiddel enkel op indirecte wijze kan worden uitgeoefend.

Het Hof geeft hierop een genuanceerd antwoord. Het Hof bevestigt in de zaak Rotaru dat: « en matière de surveillance secrète, un mécanisme objectif de contrôle peut être suffisant aussi longtemps que les mesures restent secrètes. Ce n'est qu'une fois les mesures divulguées que des voies de recours doivent s'ouvrir à l'individu »¹⁰³. Het indirect rechtsmiddel in het Belgisch systeem betreft zowel de geheime gegevens als de gegevens die verder worden verspreid (bv ten gevolge van een strafrechtelijke procedure). Anders gezegd, wanneer een persoon de zekerheid heeft dat de politie foute persoonlijke gegevens heeft gebruikt, kan zij bijna nooit de garantie krijgen dat deze gegevens werden verbeterd.

Het Comité van de Ministers van de Raad van Europa nam op 17 september 1987 een aanbeveling, de Aanbeveling R (87) 15 over het gebruik van persoonsgegevens op het terrein van de politie, waarin bepaalde vereisten gesteld worden aan het recht op toegang, verbetering en verwijdering van gegevens:

« 6.4. De uitoefening van het recht van toegang, verbetering en verwijdering mag slechts worden beperkt voor zover die beperking onontbeerlijk is voor de uitoefening van de wettelijke taak van de politie »;

⁹⁹ Zie o. a. EHRM, Çakıcı it. Turkije [GC], nr. 23657/94, § 112.

¹⁰⁰ EHRM, Rotaru eerder geciteerd, § 67.

¹⁰¹ EHRM, Friedl t. Oostenrijk, 19 mei 1994.

¹⁰² Art 43 van het KB van 13 februari 2001.

¹⁰³ EHRM, Rotaru eerder geciteerd, § 69 en Klass eerder geciteerd, p. 31, §§ 70-71.

« 6.5. Weigering of beperking van deze rechten dient schriftelijk met redenen te worden omkleed. Weigering redenen op te geven is slechts toegestaan voor zover dit onontbeerlijk is voor de uitoefening van de wettelijke politietaak ».

In het Belgisch systeem is de beperking de bijna absolute regel die wordt gerechtvaardigd door de noodzaak om het geheim van het onderzoek te respecteren.

Volgens de wetgever « zou het immers paradoxaal zijn aan de daders of de mededaders dan wel aan de medeplechtigen aan strafrechtelijke misdrijven de mogelijkheid te bieden voorafgaandelijk aan de tenlastelegging inlichtingen in te winnen omtrent het bewijsmateriaal dat de autoriteiten tegen hen hebben verzameld »¹⁰⁴. Nochtans, is deze rechtvaardiging niet van toepassing alle persoonsgegevens die worden verzameld buiten een strafonderzoek.

Het Hof stelt: « d'après la jurisprudence de la Convention, un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'État peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme »¹⁰⁵. Het Belgisch mechanisme voorziet in een algemene weigering tot toegang in alle gevallen, zelfs voor deze gevallen waar een toegang tot de gegevens geen invloed zou hebben op de efficiëntie van het toezichtstelsel. Men kan dus ernstig twijfelen of het systeem van een indirect rechtsmiddel verenigbaar is met de artikelen 8 en 13 van het EVRM.

Een andere nog meer cruciale vraag is: kan men nog redelijkerwijze stellen dat een rechtsmiddel daadwerkelijk is « zowel in rechte als in de praktijk »¹⁰⁶, wanneer het resultaat volledig geheim blijft, wat in de Belgische procedure het geval is.

Besluit

In tegenstelling tot wat men kan beweren, moet met niet “iets te verbergen hebben” om het recht op zijn privéleven gerespecteerd te zien. Dit geldt evenzeer, zelfs nog meer, voor wat betreft de fichering door politie. We hebben het reeds gezien, een foutieve fichering of een verkeerde interpretatie ervan kan leiden tot een « vals positief » resultaat. Deze fout kan op zijn beurt leiden tot zware inbreuken op andere vrijheden, zoals de onmogelijkheid om te reizen of zelfs een arrestatie. De weigering van een tewerkstelling kan ook een gevolg zijn van een foute fichering. De technologie laat toe dat complexe en gevoelige informatie gemakkelijk behandeld en verwerkt wordt. De versterking van de samenwerking van politie en strafrecht, zowel op Europees en internationaal niveau, vermenigvuldigt het aantal transfers en dus het risico op problematische verwerking van gegevens. Door de principes van de “directe beschikbaarheid” en het « wederzijds vertrouwen », kan een ongerechtvaardigde fichering zware en schadelijke gevolgen hebben in de gehele Europese Unie en misschien zelfs daarbuiten¹⁰⁷.

¹⁰⁴ Ch., Doc. Parl., 1610/1, 90/91, p. 17 en verslag aan de Koning door de toenmalige Minister van Justitie Marc Verwilghen, voor het KB van 13 februari 2001 (MB 13 maart 2001, p 7868).

¹⁰⁵ EHRM Segerstedt-Wiberg en anderen t. Zweden van 6 juni 2006, § 102, verwijzend naar Klass en anderen, § 58, en Leander, § 66.

¹⁰⁶ EHRM, arrest Wille t. Liechtenstein [GC], no 28396/95, § 75.

¹⁰⁷ Zie het interessant voorbeeld van het koppel Moon (van de bekende sekte); zij werden in het Schengeninformatiesysteem gesignaleerd gedurende meer dan 10 jaar, en hebben verschillende beroepen in een aantal landen van de EU moeten indienen, waaronder België (Evelien BROUWER, « The Other Side of Moon. The Schengen Information System and Human Rights: A Task for National Courts », CEPS Working document n° 288 / April 2008, <http://www.ceps.eu>)

De politiek om de politie "carte blanche" te geven voor het beheer van deze databanken is niet enkel bedreigend voor het privéleven op zich. Door het negeren van het respect voor het privé-leven loopt men het risico op een domino-effect, waarbij ook andere fundamentele rechten worden geschonden.

Wanneer de regels worden uitgewerkt voor het beheer van gegevens door politie, en in het bijzonder de bewaartermijn, moeten verdedigers van de mensenrechten en burgers die de bezorgd zijn om hun vrijheden de handen in elkaar slaan. Zij moeten zeer waakzaam en vooruitdenkend zijn, vermits dit dossier voor het parlement komt. Dit moment zal zonder twijfel de gelegenheid geven om aan te dringen op stevige garanties voor de burgers die het voorwerp van een eventuele fichage kunnen uitmaken. En zo kan misschien ook worden voorkomen dat België veroordeeld wordt door internationale instanties...

*Mathieu Beys dankt iedereen die geholpen heeft
met de voorbereiding en met de vertaling van deze tekst'.*

Bijlagen

- 1) Een paar relevante wetteksten
- 2) Aangifte ANG bestuurpolitie
- 3) Modelbrief recht op toegang onrechtstreeks

BIJLAGE 1: EEN PAAR RELEVANTE WETTEKSTEN

Wet van 5 augustus 1992 op het politieambt

Onderafdeling 3. - (Het informatiebeheer). <Ingevoegd bij W 1998-12-07/31, art. 191; Inwerkingtreding : 01-01-2001 >

Art. 44/1. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding**: 01-01-2001 > Bij het vervullen van de opdrachten die hun zijn toevertrouwd, kunnen de politiediensten gegevens van persoonlijke aard en inlichtingen inwinnen en verwerken, meer bepaald met betrekking tot de gebeurtenissen, de groeperingen en de personen die een concreet belang vertonen voor de uitoefening van hun opdrachten van bestuurlijke politie en voor de uitoefening van hun opdrachten van gerechtelijke politie overeenkomstig de artikelen 28bis, 28ter, 55 en 56 van het Wetboek van Strafvordering.

(Bij het vervullen van hun opdrachten van gerechtelijke en van bestuurlijke politie kunnen de politiediensten op de wijze bepaald door de Koning, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de persoonsgegevens verzamelen en verwerken bedoeld in artikel 6 van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.) <W 2001-04-02/34, art. 4, 007; **Inwerkingtreding**: 01-01-2001 >

(Deze gegevens en inlichtingen kunnen enkel worden medegedeeld aan de overheden bedoeld in artikel 5, de (Belgische of buitenlandse) politiediensten, (de Dienst Enquêtes van het Vast Comité P, de Dienst Enquêtes van het Vast Comité I, (het Coördinatieorgaan voor de dreiginganalyse,)) de algemene inspectie van de federale politie en van de lokale politie evenals aan de inlichtingen- en veiligheidsdiensten (bij het Vast Comité P en bij het Vast Comité I) die ze nodig hebben voor de uitoefening van hun opdrachten.) (Ze kunnen eveneens medegedeeld worden aan internationale organisaties voor politionele samenwerking ten aanzien waarvan de Belgische openbare overheden of politiediensten verplichtingen hebben.) <W 2001-04-02/34, art. 4, 007; **Inwerkingtreding**: 01-01-2001 > <W 2002-04-26/30, art. 134, 008; **Inwerkingtreding**: 30-04-2002 > <W 2003-05-03/59, art. 17, 010; **Inwerkingtreding**: 01-07-2003 > <W 2006-07-10/32, art. 16, 013; Inwerkingtreding : onbepaald en ten laatste : 01-12-2006 >

(De Koning bepaalt naar welke andere publieke autoriteiten dezelfde gegevens en informatie eveneens mogen medegedeeld worden door een besluit vastgesteld na overleg in de Ministerraad die de modaliteiten ervan bepaalt na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.) <W 2002-04-26/30, art. 134, 008; **Inwerkingtreding**: 30-04-2002 >

(De Koning bepaalt de gegevens en informatie die eveneens mogen worden meegedeeld aan DE POST, onverminderd de toepassing van artikel 13, § 3, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven, met het oog op de administratieve behandeling van de onmiddellijke inningen, bij een besluit vastgesteld na overleg in de Ministerraad dat de modaliteiten van deze gegevensoverdracht bepaalt na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.) <W 2005-12-27/31, art. 10, 010; Inwerkingtreding : 09-01-2006 >

Art. 44/2. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> Het inwinnen, de verwerking en het toezenden van de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, gebeurt overeenkomstig de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Deze inlichtingen en gegevens moeten in rechtstreeks verband staan met de bestaansreden van het gegevensbestand en beperkt blijven tot de vereisten die eruit voortvloeien.

(Lid 2 opgeheven) <W 2001-04-02/34, art. 5, 007; **Inwerkingtreding:** 01-01-2001>

Binnen de politiediensten worden contactpersonen voor de Commissie voor de Bescherming van de Persoonlijke Levenssfeer aangewezen.

(Het beheer van de informaticatechnische structuren en middelen, nodig voor de algemene nationale gegevensbank, bedoeld in artikel 44/4, gebeurt door het commissariaat-generaal van de federale politie.) <W 2006-06-20/34, art. 6, 014; **Inwerkingtreding:** 01-03-2007>

Art. 44/3. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> De inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, met betrekking tot de opdrachten van bestuurlijke politie worden ingewonnen en verwerkt onder het gezag van de minister van Binnenlandse Zaken.

Onverminderd de eigen bevoegdheden van de gerechtelijke overheden, worden de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, met betrekking tot de opdrachten van gerechtelijke politie ingewonnen en verwerkt onder het gezag van de minister van Justitie.

Art. 44/4. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> De inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, worden, volgens de modaliteiten bepaald door de Koning bij een in Ministerraad overlegd besluit, verwerkt in een algemene nationale gegevensbank, opgericht binnen (het commissariaat-generaal van de federale politie). (In die modaliteiten wordt hoofdzakelijk de duur van de bewaring van voornoemde inlichtingen en gegevens bepaald.) In deze gegevensbank zijn meerdere indexsystemen vervat. In het kader van deze indexsystemen, regelt de Koning ook het toezicht van (het controleorgaan bedoeld in artikel 44/7) over de gerechtelijke informatie. <W 2001-04-02/34, art. 6, 007; **Inwerkingtreding:** 01-01-2001> De Koning bepaalt, bij een in Ministerraad overlegd besluit, de voorwaarden waaronder deze gegevensbank en elk van deze indexsystemen toegankelijk en bevragebaar zijn door de bevoegde gerechtelijke overheden en de politiediensten in het kader van de uitoefening van hun opdrachten. <W 2006-06-20/34, art. 7, 014; **Inwerkingtreding:** 01-03-2007>

De politiediensten zenden ambtshalve en rechtstreeks de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, aan deze algemene nationale gegevensbank toe.

De ministers van Binnenlandse Zaken en van Justitie bepalen, elk binnen het kader van zijn bevoegdheden, op eensluidend advies van het controleorgaan bedoeld in artikel 44/7, de categorieën van inlichtingen en gegevens die geen toezending vereisen.

Art. 44/5. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> Wanneer de politiediensten in het kader van de uitoefening van hun opdrachten van bestuurlijke politie kennis krijgen van informatie die voor de uitoefening van de gerechtelijke politie van belang is, stellen zij daarvan onverwijld en zonder enige beperking de bevoegde gerechtelijke overheden in kennis.

Wanneer de politiediensten in het raam van de uitoefening van hun opdrachten van gerechtelijke politie kennis krijgen van informatie die voor de uitoefening van de bestuurlijke politie van belang is en aanleiding kan geven tot beslissingen van bestuurlijke politie, stellen zij daarvan, behoudens wanneer dit

de uitoefening van de strafvordering in het gedrang kan brengen, maar onverminderd de voor de bescherming van personen noodzakelijke maatregelen, de bevoegde bestuurlijke overheden in kennis.

Art. 44/6. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> Bij de uitvoering van hun opdrachten van gerechtelijke politie delen de politiediensten de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid, aan de bevoegde gerechtelijke overheden mee, overeenkomstig wat is bepaald bij de artikelen 28bis, 28ter, 55 en 56 van het Wetboek van Strafvordering.

Art. 44/7. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding:** 01-01-2001> Er wordt een controleorgaan opgericht onder het gezag van de minister van Binnenlandse Zaken en van de minister van Justitie, belast met de (controle op de verwerking van de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid). Dit controleorgaan heeft een onbeperkt recht op toegang tot alle inlichtingen en gegevens bewaard in deze gegevensbank. <W 2001-04-02/34, art. 7, 007; **Inwerkingtreding:** 01-01-2001>

Het is in het bijzonder belast met de controle van de naleving van de regels inzake de toegankelijkheid van de algemene nationale gegevensbank en de toezending aan deze gegevensbank van de inlichtingen en gegevens bedoeld in artikel 44/1, eerste lid.

Onverminderd de bepalingen van artikel 44/4, kunnen de politiediensten in bijzondere omstandigheden gegevensbanken oprichten. De oprichting van elke gegevensbank door de politiediensten, dient voorafgaandelijk aan dit controleorgaan te worden gemeld. Alle inlichtingen en gegevens in deze gegevensbanken worden aan de algemene nationale gegevensbank bedoeld in artikel 44/4, eerste lid, meegedeeld, behalve wanneer er een akkoord is van het controleorgaan met een verzoek tot niet-mededeling. Ten aanzien van deze gegevensbanken gelden onverkort alle bevoegdheden van het controleorgaan, zoals vermeld in dit artikel. Onder de voorwaarden bepaald door de Koning, bij een in Ministerraad overlegd besluit, zijn deze gegevensbanken toegankelijk en bevragebaar door de bevoegde overheden, elk binnen het kader van hun bevoegdheden, en de politiediensten in het kader van de uitoefening van hun opdrachten.

Teneinde zijn controleopdrachten te kunnen vervullen, heeft dit orgaan een onbeperkt recht op toegang tot de lokalen waarin en gedurende de tijd dat de politieambtenaren er hun functies uitoefenen.

Dit orgaan wordt voorgezeten door een federale magistraat. Deze magistraat wordt door de minister van Justitie en de minister van Binnenlandse Zaken aangewezen, (op voorstel van de federale procureur). Hij handelt voor de duur van zijn aanwijzing onafhankelijk ten aanzien van het federaal parket. Voor het overige is dit orgaan samengesteld uit een lid van de lokale politie, een lid van de federale politie en een deskundige, die door de minister van Binnenlandse Zaken en de minister van Justitie worden aangewezen. (In geval van afwezigheid hebben de voorzitter en de leden bovendien elk een plaatsvervanger, aangewezen overeenkomstig de respectieve procedures van de werkende leden.) <W 2001-04-02/34, art. 7, 007; **Inwerkingtreding:** 01-01-2001>

Het controleorgaan treedt ambtshalve op al op verzoek van de gerechtelijke of bestuurlijke overheden, van de minister van Justitie of van de minister van Binnenlandse Zaken, overeenkomstig de voorwaarden bepaald door de Koning bij een in Ministerraad overlegd besluit.

Wanneer de controle heeft plaatsgevonden binnen een lokale politie, informeert het controleorgaan daar de burgemeester of het politiecollege van en zendt hem zijn verslag.

Wanneer de controle inlichtingen en gegevens betreft die verband houden met de uitoefening van opdrachten van gerechtelijke politie, wordt het verslag dat dienaangaande door het controleorgaan wordt opgesteld, ook aan de procureur des Konings toegezonden.

Dit controleorgaan wordt logistiek en administratief ondersteund door de algemene inspectie van de federale politie en van de lokale politie en kan, voor de uitvoering van haar opdracht, de bijstand vorderen van deze inspectie.

De Koning bepaalt, bij een in Ministerraad overlegd besluit, de regels met betrekking tot het statuut van de leden (en van hun plaatsvervangers) van dit controleorgaan derwijze dat hun onafhankelijkheid wordt gewaarborgd. <W 2001-04-02/34, art. 7, 007; **Inwerkingtreding**: 01-01-2001>

Art. 44/8. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding**: 01-01-2001> In afwijking van artikel 44/4 wordt de toezending bedoeld in artikel 44/4, derde lid, uitgesteld wanneer en tot zolang de bevoegde magistraat in akkoord met de (federale procureur), van oordeel is dat deze toezending de uitoefening van de strafvordering of de veiligheid van een persoon in gevaar kan brengen. <W 2001-04-02/34, art. 8, 007; **Inwerkingtreding**: 01-01-2001>

Art. 44/9. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding**: 01-01-2001> De politieambtenaren belast met het beheer van de algemene nationale gegevensbank bedoeld in artikel 44/4, eerste lid, worden aangewezen na advies van het controleorgaan bedoeld in artikel 44/7. Geen enkele bevordering, benoeming of mutatie kan hen worden toegekend dan op initiatief of met het akkoord van de bevoegde minister, en na advies van dit controleorgaan. De nadere regels hiervan worden bepaald door de Koning.

Ten aanzien van deze politieambtenaren kan een tuchtrechtelijke procedure voor feiten gepleegd tijdens de duur van de aanwijzing slechts worden ingesteld met instemming of op bevel van de bevoegde minister. Het advies van het controleorgaan wordt ingewonnen voor tuchtprocedures die niet door de minister worden bevolen.

De algemene nationale gegevensbank bedoeld in artikel 44/4, eerste lid, wordt beheerd in een dienst die onder leiding staat van een diensthoofd en een adjunct-diensthoofd. Eén van beide behoort tot de federale politie en de andere behoort tot de lokale politie. De nadere regels van hun aanwijzing worden door de Koning bepaald.

Art. 44/10. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding**: 01-01-2001> De uitvoeringsmaatregelen bedoeld in de artikelen (...)44/4, tweede lid en 44/7, derde en negende lid, worden genomen na advies van de Commissie voor de Bescherming van de Persoonlijke Levenssfeer, uitgezonderd in geval van hoogdringendheid. <W 2001-04-02/34, art. 9, 007; **Inwerkingtreding**: 01-01-2001>

Art. 44/11. <Ingevoegd bij W 1998-12-07/31, art. 191; **Inwerkingtreding**: 01-01-2001> Elke politieambtenaar die willens en wetens inlichtingen en gegevens die van belang zijn voor de uitoefening van de strafvordering of de handhaving van de openbare orde achterhoudt en nalaat door te zenden aan de algemene nationale gegevensbank overeenkomstig artikel 44/4, derde lid, wordt gestraft met gevangenisstraf van één maand tot zes maanden en een geldboete van zesentwintig tot vijfhonderd frank of met één van die straffen alleen.

De bepalingen van boek I van het Strafwetboek. hoofdstuk VII en artikel 85 niet uitgezonderd, zijn toepasselijk op dit misdrijf.

Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens

Geconsolideerde versie (01/08/2007)

http://www.privacycommission.be/nl/static/pdf/wetgeving/wet_privacy_08_12_1992.pdf

Art 3 § 5. De artikelen 9, 10, § 1, en 12 zijn niet van toepassing :

1° op de verwerkingen van persoonsgegevens beheerd door openbare overheden met het oog op de uitoefening van hun opdrachten van gerechtelijke politie;

2° op de verwerkingen van persoonsgegevens beheerd door de politiediensten bedoeld in artikel 3 van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, met het oog op de uitoefening van hun opdrachten van bestuurlijke politie;

3° op de verwerkingen van persoonsgegevens beheerd, met het oog op de uitoefening van hun opdrachten van bestuurlijke politie, door andere openbare overheden die aangewezen zijn bij een in Ministerraad overlegd koninklijk besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer;

4° op de verwerkingen van persoonsgegevens die noodzakelijk zijn geworden ten gevolge van de toepassing van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld;

5° op de verwerking van persoonsgegevens beheerd door het Vast Comité van Toezicht op de politiediensten en de Dienst Enquêtes ervan met het oog op de uitoefening van hun wettelijke opdrachten.

(...)

Hoofdstuk III. Rechten van de betrokkene

Art. 9. § 1.

Indien persoonsgegevens betreffende de betrokkene bij hemzelf worden verkregen, moet de verantwoordelijke voor de verwerking of diens vertegenwoordiger uiterlijk op het moment dat de gegevens worden verkregen aan de betrokkene ten minste de hierna volgende informatie verstrekken, behalve indien hij daarvan reeds op de hoogte is :

- a) de naam en het adres van de verantwoordelijke voor de verwerking en, in voorkomend geval, van diens vertegenwoordiger;
- b) de doeleinden van de verwerking;
- c) het bestaan van een recht om zich op verzoek en kosteloos tegen de voorgenomen verwerking van hem betreffende persoonsgegevens te verzetten, indien de verwerking verricht wordt met het oog op direct marketing;
- d) andere bijkomende informatie, met name:
 - de ontvangers of de categorieën ontvangers van de gegevens,
 - het al dan niet verplichte karakter van het antwoord en de eventuele gevolgen van niet-beantwoording,

- het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem betrekking hebben; behalve indien die verdere informatie, met inachtneming van de specifieke omstandigheden waaronder de persoonsgegevens verkregen worden, niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen;
- e) andere informatie afhankelijk van de specifieke aard van de verwerking, die wordt opgelegd door de Koning na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

§ 2. Indien de persoonsgegevens niet bij de betrokkene zijn verkregen, moet de verantwoordelijke voor de verwerking of zijn vertegenwoordiger, op het moment van de registratie van de gegevens of wanneer mededeling van de gegevens aan een derde wordt overwogen, uiterlijk op het moment van de eerste mededeling van de gegevens, ten minste de volgende informatie verstrekken, tenzij de betrokkene daarvan reeds op de hoogte is:

- a) de naam en het adres van de verantwoordelijke voor de verwerking en, in voorkomend geval, van diens vertegenwoordiger;
- b) de doeleinden van de verwerking;
- c) het bestaan van een recht om zich op verzoek en kosteloos tegen de voorgenomen verwerking van hem betreffende persoonsgegevens te verzetten, indien de verwerking verricht wordt met het oog op direct marketing; in dit geval dient de betrokkene in kennis te worden gesteld vooraleer de persoonsgegevens voor de eerste keer aan een derde worden verstrekt of voor rekening van derden worden gebruikt voor direct marketing;
- d) andere bijkomende informatie, met name :
 - de betrokken gegevenscategorieën;
 - de ontvangers of de categorieën ontvangers;
 - het bestaan van een recht op toegang en op verbetering van de persoonsgegevens die op hem betrekking hebben; behalve indien die verdere informatie, met inachtneming van de specifieke omstandigheden waaronder de gegevens verwerkt worden, niet nodig is om tegenover de betrokkene een eerlijke verwerking te waarborgen;
- e) andere informatie afhankelijk van de specifieke aard van de verwerking, die wordt opgelegd door de Koning na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer.

De verantwoordelijke voor de verwerking wordt van de in deze paragraaf bedoelde kennisgeving vrijgesteld:

- a) wanneer, met name voor statistische doeleinden of voor historisch of wetenschappelijk onderzoek of voor bevolkingsonderzoek met het oog op de bescherming en de bevordering van de volksgezondheid, de kennisgeving aan de betrokkene onmogelijk blijkt of onevenredig veel moeite kost;
- b) wanneer de registratie of de verstrekking van de persoonsgegevens verricht wordt met het oog op de toepassing van een bepaling voorgeschreven door of krachtens een wet, een decreet of een ordonnantie. De Koning bepaalt bij een in Ministerraad overlegd besluit na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer de voorwaarden voor de toepassing van het vorige lid. Indien de eerste mededeling van de gegevens geschiedde vóór de inwerkingtreding van deze bepaling, moet de mededeling van de informatie, in afwijking van het eerste lid, uiterlijk geschieden binnen een termijn van 3 jaar vanaf de datum van inwerkingtreding van deze bepaling. De informatie moet evenwel niet worden meegedeeld indien de verantwoordelijke voor de verwerking was vrijgesteld van de verplichting om de betrokkene in kennis te stellen van de registratie van de

gegevens krachtens de wettelijke en reglementaire bepalingen van toepassing op de dag voorafgaand aan de datum van inwerkingtreding van deze bepaling.

Art. 10. § 1. De betrokkene die zijn identiteit bewijst, heeft het recht om vanwege de verantwoordelijke voor de verwerking te verkrijgen :

- a) kennis van het al dan niet bestaan van verwerkingen van hem betreffende gegevens alsmede ten minste informatie over de doeleinden van deze verwerkingen, van de categorieën gegevens waarop deze verwerkingen betrekking hebben en van de categorieën ontvangers aan wie de gegevens worden verstrekt;
- b) verstrekking in begrijpelijke vorm van de gegevens zelf die worden verwerkt, alsmede alle beschikbare informatie over de oorsprong van die gegevens;
- c) mededeling van de logica die aan een geautomatiseerde verwerking van hem betreffende gegevens ten grondslag ligt in geval van geautomatiseerde besluitvorming in de zin van artikel 12bis;
- d) kennis van de mogelijkheid om de in de artikelen 12 en 14 bedoelde beroepen in te stellen en eventueel inzage te nemen van het in artikel 18 bedoelde openbaar register. Daartoe richt de betrokkene een gedagtekend en ondertekend verzoek aan de verantwoordelijke voor de verwerking of aan iedere andere persoon die de Koning aanwijst. De inlichtingen worden onverwijld en ten laatste binnen vijfenveertig dagen na ontvangst van het verzoek meegedeeld. De Koning kan nadere regels voor de uitoefening van het in het eerste lid bedoelde recht bepalen.

(...)

Art. 13. Eenieder die zijn identiteit bewijst, is gerechtigd zich kosteloos tot de Commissie voor de bescherming van de persoonlijke levenssfeer te wenden, teneinde de in de artikelen 10 en 12 bedoelde rechten uit te oefenen ten aanzien van de verwerkingen van persoonsgegevens bedoeld in artikel 3, paragrafen 4, 5 en 6.

De Koning bepaalt, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en bij een in Ministerraad overlegd besluit, de wijze waarop deze rechten worden uitgeoefend.

De Commissie voor de bescherming van de persoonlijke levenssfeer deelt uitsluitend aan de betrokkene mede dat de nodige verificaties werden verricht.

Evenwel bepaalt de Koning, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, bij een in Ministerraad overlegd besluit, welke informatie de Commissie aan de betrokkene mag medelen indien het verzoek van de betrokkene een verwerking van persoonsgegevens betreft door politiediensten met het oog op identiteitscontrole.

Art. 14. § 1. De voorzitter van de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, neemt kennis van de vorderingen betreffende het door of krachtens de wet verleende recht om kennis te krijgen van persoonsgegevens, alsook van de vorderingen tot verbetering, tot verwijdering of tot het verbieden van de aanwending van onjuiste persoonsgegevens of die gelet op het doel van de verwerking onvolledig of niet ter zake dienend zijn, dan wel waarvan de registratie de mededeling of de bewaring verboden is, tegen de verwerking waarvan de betrokkene zich heeft verzet of die langer bewaard werden dan de toegestane duur.

§ 2. De voorzitter van de rechtbank van de woonplaats van de eiser is bevoegd voor de in § 1 bedoelde vorderingen. Indien de eiser geen woonplaats in België heeft, is de voorzitter van de rechtbank van de

woonplaats van de verantwoordelijke voor de verwerking, die een natuurlijke persoon is, bevoegd. Indien de verantwoordelijke voor de verwerking een rechtspersoon is, is de voorzitter van de rechtbank van de maatschappelijke of administratieve zetel bevoegd.

De beschikking wordt in openbare rechtszitting uitgesproken. Zij is uitvoerbaar bij voorraad, niettegenstaande hoger beroep of verzet.

§ 3. De vordering wordt ingediend bij verzoekschrift op tegenspraak.

Het verzoekschrift vermeldt op straffe van nietigheid :

1° de dag, de maand en het jaar;

2° de naam, de voornaam, het beroep en de woonplaats van de eiser;

3° de naam, de voornaam en de woonplaats van de op te roepen persoon;

4° het voorwerp van de vordering en de korte samenvatting van de middelen;

5° de handtekening van de eiser of van zijn advocaat.

§ 4. Het verzoekschrift wordt bij ter post aangetekende brief toegezonden aan de griffier van het gerecht of ter griffie neergelegd.

Nadat, in voorkomend geval de rolrechten zijn betaald, worden de partijen door de griffier bij gerechtsbrief opgeroepen om te verschijnen op de zitting die de rechter bepaalt. Bij de oproeping wordt een afschrift van het verzoekschrift gevoegd.

§ 5. De op grond van § 1 ingestelde vordering is pas ontvankelijk als het verzoek, bedoeld in artikel 10, § 1, of dat bedoeld in artikel 12, § 2, is afgewezen of als daaraan naargelang het geval, binnen de door artikel 10, § 1, tweede lid dan wel door artikel 12, § 3, eerste lid, voorgeschreven termijn geen gevolg is gegeven.

§ 6. Indien onjuiste, onvolledige of niet ter zake dienende gegevens of gegevens waarvan de bewaring verboden is aan derden zijn medegedeeld, dan wel wanneer een mededeling van gegevens heeft plaatsgehad na verloop van de tijd waarin de bewaring van die gegevens toegelaten is, kan de voorzitter van de rechtbank gelasten dat de verantwoordelijke voor de verwerking aan die derden van de verbetering of de verwijdering van die gegevens kennis geeft.

§ 7. Wanneer dwingende redenen de vrees doen rijzen dat bewijsmateriaal dat kan worden aangevoerd bij een in § 1 bedoelde vordering zou kunnen worden verheeld of verdwijnen, gelast de voorzitter van de rechtbank van eerste aanleg op eenzijdig verzoekschrift, ondertekend en ingediend door de partij of haar advocaat, elke maatregel ter voorkoming van die verheling of verdwijning.

§ 8. De bepalingen van de §§ 6 en 7 houden geen beperking in van de algemene bevoegdheid ter zake van de voorzitter van de rechtbank van eerste aanleg, zetelend in kort geding.

Art. 15. Onmiddellijk bij het ontvangen van het verzoek tot verbetering, verwijdering of verbod van gebruik of bekendmaking van persoonsgegevens of bij de kennisgeving van de instelling van het geding bedoeld in artikel 14 en tot een beslissing in kracht van gewijsde is getreden, dient de verantwoordelijke voor de verwerking bij elke mededeling van een persoonsgegeven duidelijk aan te geven dat het gegeven betwist is.

Art. 15bis. Indien een betrokkene schade lijdt doordat ten opzichte van hem in strijd wordt gehandeld met de bij of krachtens deze wet bepaalde voorschriften, zijn het hiernavolgende tweede en derde lid van toepassing, onverminderd de aanspraken op grond van andere wettelijke regels.

De verantwoordelijke voor de verwerking is aansprakelijk voor de schade die voortvloeit uit een handeling in strijd met de bij of krachtens deze wet bepaalde voorschriften.

Hij is van deze aansprakelijkheid ontheven indien hij bewijst dat het feit dat de schade heeft veroorzaakt hem niet kan worden toegerekend.

Koninklijk besluit van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens

HOOFDSTUK VI. - Uitoefening van het recht bedoeld in artikel 13 van de wet.

Art. 36. Dit hoofdstuk bepaalt de procedure voor de indiening van verzoeken op grond van artikel 13 van de wet.

Art. 37. De betrokken persoon dient het verzoek bij de Commissie in aan de hand van een gedagtekend en ondertekend schrijven waarin zijn naam, voornaam, geboortedatum en nationaliteit zijn vermeld en waarbij een fotokopie is gevoegd van zijn identiteitskaart, van zijn paspoort of van het daarmee gelijkgestelde document.

In het verzoek, worden tevens volgende gegevens vermeld indien de verzoeker daarover beschikt :

- de naam van de betrokken overheid of dienst;
- alle relevante elementen betreffende de betwiste gegevens, zoals de aard ervan, de omstandigheden of de aanleiding van de kennisneming ervan, alsook de eventueel gewenste verbeteringen.

Art. 38. Indien de Commissie zulks nuttig acht, kan zij aan de betrokken persoon bijkomende inlichtingen vragen.

Art. 39. Indien de gegevens, bedoeld in de artikelen 37 en 38 van dit besluit, niet worden meegedeeld, kan het verzoek als niet-ontvankelijk worden beschouwd.

Art. 40. Het verzoek is niet-ontvankelijk wanneer het wordt ingediend binnen een termijn van een jaar te rekenen van de verzendingsdatum van het vorige antwoord van de Commissie betreffende dezelfde gegevens en dezelfde diensten.

Van die termijn kan worden afgeweken ingeval de betrokken persoon in zijn verzoek redenen ter staving van die afwijking aanvoert.

Art. 41. Wanneer het verzoek als niet-ontvankelijk wordt beschouwd, wordt de betrokken persoon daarvan per brief in kennis gesteld.

In dit schrijven wordt vermeld dat de betrokken persoon op verzoek wordt gehoord, zulks eventueel bijgestaan door zijn raadsman.

Art. 42. De controle bij de betrokken dienst wordt verricht door de voorzitter van de Commissie of door een of meer leden ervan die hij aanwijst.

De controle op de verwerkingen van persoonsgegevens, bedoeld in artikel 3, § 5, 1°, van de wet, wordt verricht door magistraten die de Commissie in haar midden aanwijst.

De voorzitter en de leden die de controle verrichten, kunnen zich laten bijstaan of vertegenwoordigen door een of meer leden van het secretariaat van de Commissie.

Art. 43. In het kader van de controle bij de betrokken dienst verricht of beveelt de Commissie alle verificaties die zij nuttig acht.

Ter gelegenheid van de controle uitgeoefend bij de betrokken dienst bedoeld in artikel 3, § 5, van de wet, kan ze gegevens doen verbeteren of verwijderen, of gegevens doen invoeren die verschillen van die welke de betrokken dienst verwerkt. Zij kan de mededeling van de gegevens te verbieden.

Ter gelegenheid van de controle uitgeoefend bij de betrokken dienst bedoeld in artikel 3, § 4, van de wet, beveelt de Commissie de maatregelen aan die ze noodzakelijk acht. Zij motiveert haar aanbevelingen.

Art. 44. De betrokken dienst geeft na die verificaties aan de Commissie schriftelijk kennis van het gevolg dat eraan is gegeven.

Art. 45. De Commissie antwoordt per brief op het verzoek van de betrokken persoon binnen een termijn van drie maanden te rekenen van de kennisgeving bedoeld in het artikel 44 van dit besluit.

Art. 46. Ingeval het verzoek van de betrokken persoon betrekking heeft op een verwerking van persoonsgegevens beheerd door een politiedienst met het oog op een identiteitscontrole, deelt de Commissie aan die persoon mee dat de nodige verificaties zijn verricht.

In voorkomend geval, verstrekt de Commissie, na advies van de betrokken dienst, aan de betrokken persoon alle andere inlichtingen die zij relevant acht.

BIJLAGE 2: AANGIFTE ANG BESTUURPOLITIE

DEEL 1. Verantwoordelijke voor de verwerking



Naam (of benaming rechtspersoon, feitelijke vereniging of openbaar bestuur)

Le Ministre de l'Intérieur

Adres:

de la loi 2

1000 BRUXELLES

België

Juridisch statuut van de verantwoordelijke voor de verwerking

- *Openbaar bestuur*

- *Politiedienst*

DEEL 2. De verwerking



1. Benaming van de verwerking

Banque de données Nationale Générale-traitements de police administrative

2. Doel of geheel van samenhangende doeleinden waarvoor gegevens worden verwerkt

- Opdrachten van bestuurlijke politie

3. Categorieën van gegevens die verwerkt worden

- Identificatiegegevens (naam, adres, tel, ...)
- Elektronische identificatiegegevens (IP-adressen, cookies, ...)
- Elektronische lokalisatiegegevens (GSM, GPS,,,,)
- Biometrische identificatiegegevens
- Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, ...)
- Lidmaatschappen
- Beroep en betrekking
- Beeldopnamen
- Rijksregisternummer/identificatienummer van de sociale zekerheid
- Raciale of etnische gegevens
- Politieke opvattingen
- Filosofische of religieuze overtuigingen
- Veroordelingen en straffen
- Gerechtelijke maatregelen
- Administratieve sancties

4. Wettelijke of reglementaire basis(sen)

Wet, decreet, ordonnantie, KB of besluit van 05/08/1992

Titel *loi sur la fonction de police, articles 44/1 et suivants*

Wet, decreet, ordonnantie, KB of besluit van 08/12/1992

Titel *loi relative à la protection de la vie privée*

5. Categorieën ontvangers en categorieën gegevens die kunnen worden verstrekt

Gerecht en politiediensten

- Identificatiegegevens (naam, adres, tel, ...)
- Elektronische identificatiegegevens (IP-adressen, cookies, ...)
- Elektronische lokalisatiegegevens (GSM, GPS, ...)
- Biometrische identificatiegegevens
- Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, ...)
- Lidmaatschappen
- Veroordelingen en straffen
- Gerechtelijke maatregelen
- Administratieve sancties
- Beroep en betrekking
- Rijksregisternummer/identificatienummer van de sociale zekerheid
- Raciale of etnische gegevens
- Politieke opvattingen
- Filosofische of religieuze overtuigingen
- Beeldopnamen

6. Welke maatregelen zijn er genomen om de mededeling van gegevens aan derden te beveiligen ?

- Technische maatregelen (vb.crypteren, paswoorden)

7. Hoe worden de betrokken personen in kennis gesteld van de registratie van hun gegevens?

Persoonsgegevens worden verwerkt zonder dat de betrokkene in kennis moet worden gesteld

- *Ik ben vrijgesteld van kennisgeving, want de verwerking wordt, in toepassing van art.3, §5 WVP, beheerd met het oog op de uitoefening van :*
Toepasselijk onderdeel van de bepaling: 3§5, 2° LVP

8. Tot wie kunnen de geregistreerde personen zich richten om hun rechten uit te oefenen ?

Het recht op toegang van de betrokkene tot zijn gegevens en het recht om de verbetering en de verwijdering ervan te verkrijgen, worden in de art. 10-12 WVP voorzien.

Naam en voornaam (en/of naam van de dienst)

la commission de la protection de la vie privée

Adres:

haute 139

1000 BRUXELLES

Telefoon *+32 2 213 85 40*

Telefax *+32 2 213 85 65*

E-mail *commission@privacy.fgov.be*

9. Bijzondere maatregelen voor de uitoefening van de rechten

La commission de la protection de la vie privée dispose d'un point de contact au sein de la direction de la Banque de données Nationale Générale des services de police. Ce point de contact est chargé de fournir à la commission les éléments qu'elle lui demande en vertu de l'article 13 de la loi vie privée

10. Voorziene bewaartermijn

<i>Identificatiegegevens (naam, adres, tel, ...)</i>	<i>5 Jaren</i>
<i>Elektronische identificatiegegevens (IP-adressen, cookies, ...)</i>	<i>5 Jaren</i>
<i>Elektronische lokalisatiegegevens (GSM, GPS,,,,)</i>	<i>5 Jaren</i>
<i>Biometrische identificatiegegevens</i>	<i>5 Jaren</i>
<i>Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, ...)</i>	<i>5 Jaren</i>
<i>Lidmaatschappen</i>	<i>5 Jaren</i>
<i>Veroordelingen en straffen</i>	<i>5 Jaren</i>
<i>Gerechtelijke maatregelen</i>	<i>5 Jaren</i>
<i>Administratieve sancties</i>	<i>5 Jaren</i>
<i>Beroep en betrekking</i>	<i>5 Jaren</i>
<i>Rijksregisternummer/identificatienummer van de sociale zekerheid</i>	<i>5 Jaren</i>
<i>Raciale of etnische gegevens</i>	<i>5 Jaren</i>
<i>Politieke opvattingen</i>	<i>5 Jaren</i>
<i>Filosofische of religieuze overtuigingen</i>	<i>5 Jaren</i>
<i>Beeldopnamen</i>	<i>5 Jaren</i>

Indien verschillende bewaartermijnen werden geselecteerd, gelieve deze te omschrijven.

pour les exceptions, voir annexe 1

11. Algemene beschrijving van de veiligheidsmaatregelen

Algemene maatregelen genomen tot waarborg van de vertrouwelijkheid en de veiligheid van de verwerking (art.16 WVP)

Veiligheidsdienst

Maatregelen ter voorkoming van risico's

Back-up-systeem

Beveiliging en controle van de gebouwen, lokalen en apparatuur

Beveiliging van de toegang tot het systeem

Authenticatiesysteem

Loggingsysteem

Contractuele maatregelen ten aanzien van

Het personeel

Gedragscodes (aan te vullen in één van onderstaande kaders)

déontologie, respect du secret professionnel

Bijkomende verplichte veiligheidsmaatregelen te nemen bij de verwerking van persoonsgegevens bedoeld in de artikelen 6 t.e.m. 8 WVP (art. 25 en 26 KB)

Verwerking van gevoelige gegevens, gezondheidsgegevens of gerechtelijke gegevens bedoeld in de artikelen 6 tot 8 WVP

Krachtens art. 25 KB dient u te beschikken over de actuele lijst van de aangewezen categorieën personen die deze persoonsgegevens kunnen raadplegen.

Waar kan de Commissie deze lijst inzien ? (art. 25, 2° KB)

Naam en voornamen (of benaming rechtspersoon, feitelijke vereniging of openbaar bestuur)

Marc Vandendriessche (Direction de la Banque de données Nationale Générale)

Adres:

Fritz Toussaint 8

1050 BRUXELLES (IXELLES)

Telefoon +32 2 642 78 39

Telefax +32 2 642 76 38

E-mail *marc.vdd@skynet.be*

Verwerking van gevoelige gegevens of gezondheidsgegevens bedoeld in de artikelen 6 en 7 WVP, die u verricht op grond van de schriftelijke toestemming van de betrokken persoon

Verwerkt u gevoelige gegevens of gezondheidsgegevens, bedoeld in de artikelen 6 en 7 WVP op grond van de schriftelijke toestemming van de betrokken persoon?

Ja

Waar kan de Commissie deze documenten inzien ?

Naam en voornamen (of benaming rechtspersoon, feitelijke vereniging of openbaar bestuur)

x

Adres:

x

x x

Telefoon *x*

Telefax *x*

E-mail *x*

12. Gegevens die naar het buitenland worden verzonden

Alle non-Europese Unie landen

- *Identificatiegegevens (naam, adres, tel, ...)*
- *Elektronische identificatiegegevens (IP-adressen, cookies, ...)*
- *Elektronische lokalisatiegegevens (GSM, GPS,,,,)*
- *Biometrische identificatiegegevens*
- *Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, ...)*
- *Lidmaatschappen*
- *Veroordelingen en straffen*
- *Gerechtelijke maatregelen*
- *Administratieve sancties*
- *Beroep en betrekking*
- *Rijksregisternummer/identificatienummer van de sociale zekerheid*
- *Raciale of etnische gegevens*
- *Politieke opvattingen*
- *Filosofische of religieuze overtuigingen*
- *Beeldopnamen*

Alle Europese Unie landen

- *Identificatiegegevens (naam, adres, tel, ...)*
- *Elektronische identificatiegegevens (IP-adressen, cookies, ...)*
- *Elektronische lokalisatiegegevens (GSM, GPS,,,,)*
- *Biometrische identificatiegegevens*
- *Persoonlijke kenmerken (leeftijd, geslacht, burgerlijke staat, ...)*
- *Lidmaatschappen*
- *Veroordelingen en straffen*
- *Gerechtelijke maatregelen*
- *Administratieve sancties*
- *Beroep en betrekking*
- *Rijksregisternummer/identificatienummer van de sociale zekerheid*
- *Raciale of etnische gegevens*
- *Politieke opvattingen*
- *Filosofische of religieuze overtuigingen*
- *Beeldopnamen*

Indien, na de controle van de lijst opgesteld door de Europese Commissie, het land geen passend beschermingsniveau bezit, vindt de doorgifte van de persoonsgegevens toch plaats op basis van art. 22 WVP, omwille van de

- *Noodzaak of wettelijke verplichting vanwege een zwaarwegend algemeen belang of voor de vaststelling, de uitoefening of de verdediging van een recht in rechte*

BIJLAGE 3: MODEL BRIEF RECHT OP TOEGANG ONRECHTSTREEKS

CBPL
Hoogstraat 139
1000 BRUSSEL

Mijn voornaam en naam
Mijn adres
Mijn e-mailadres

Betreft: onrechtstreekse toegang tot mijn persoonsgegevens

plaats en datum

Geachte mevrouw,
Geachte heer,

Hierbij stuur ik u een verzoek om onrechtstreekse toegang tot mijn gegevens (gelieve een van onderstaande mogelijkheden te selecteren):

- ☐ in de databank van (naam van de betrokken instantie indien gekend);
- ☐ in de databank van de federale politie;
- ☐ in de databank van de Veiligheid van de Staat;
- ☐ in de databank van een andere voor mij onbekende instantie;
- ☐ in het Schengen Informatie Systeem.

Aangezien artikel 13 van de Privacywet bepaalt dat ik de gegevens die deze verantwoordelijke(n) over mij bewaart/bewaren enkel onrechtstreeks kan raadplegen, vraag ik de Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL) om dit in mijn plaats te doen. Ik ben mij ervan bewust dat de CBPL mij nadien in principe enkel zal mededelen dat de nodige verificaties werden verricht.

Conform artikel 37 van het Koninklijk Besluit ter uitvoering van de Privacywet, bezorg ik u hierbij ook de volgende gegevens:

- mijn geboortedatum:.....
- mijn nationaliteit:.....
- alle relevante elementen (bv. de aard van de gegevens, de omstandigheden van de gegevensverwerking, de reden waarom u wilt kennis nemen van uw gegevens, een eventuele betwisting of verbetering ervan):

.....
.....
.....

Als bewijs van mijn identiteit heb ik een kopie bijgevoegd van mijn identiteitskaart (of paspoort of een daarmee gelijkgesteld document).

Hoogachtend

Handtekening

Bijlage: kopie van mijn identiteitskaart/paspoort/een daarmee gelijkgesteld document

Biographie sommaire

Mathieu BEYS (° 1976), Juriste, Licencié en histoire

Expérience professionnelle

2006 - Caritas international

Conseiller juridique – rédacteur de publication

- Conseils aux travailleurs sociaux, avocats, et consultants (asile, séjour, regroupement familial, aide sociale, droit du bail, droit pénal, droit civil et judiciaire, assistance pour la rédactions d'actes de procédure, ...)
- Suivi de la législation et de la jurisprudence belge et européenne en matière d'asile et d'immigration, suivi de l'information des pays d'origine et rédaction de textes de vulgarisation destinés aux professionnels;
- Formations destinées aux travailleurs sociaux et avocats (contenu et organisation, en français, néerlandais et anglais);
- Rédacteur principal des périodiques *Parole à l'exil* et *Vluchtschrift* de Caritas international (disponible sur le site <http://www.caritas-int.be/fr/publications/parole-a-lexil.html>);
- Rédaction de textes juridiques et de communiqués pour les travailleurs sociaux et le grand public en français, néerlandais et anglais;
- Traduction de qualité de textes juridiques (doctrine, décisions judiciaires) du néerlandais et de l'anglais vers le français.

2008 - Université Libre de Bruxelles

Assistant chargé d'exercices en histoire du droit

- Professeur : Régine Beauthier
- Séances de travaux pratiques à l'attention des étudiants de 1ère année (BA 1) de la Faculté de droit

2002 - 2000 Progress Lawyers Network

Avocat au barreau de Bruxelles

- Stage clôturé et inscription au tableau de l'Ordre en 2006 ;
- Gestion de dossiers individuels sous tous les aspects (contacts clients, rédactions d'actes de procédure, négociations, plaidoiries, gestion financière du cabinet...);
- Organisation de colloques et de formations.

Formation

1996 - 2002 Université Libre de Bruxelles

Licence en droit - orientation droit public – distinction

1999 - 2001 Institut de journalisme (Association des Journalistes Professionnels)

Formation pratique en journalisme écrit et audiovisuel

Cours du soir et stage au quotidien *Le Matin* en février et mars 2001

1994 - 1999 Université Libre de Bruxelles

Licence en histoire - période contemporaine - grande distinction

Mémoire de licence: « La Parole au peuple. Presse progressiste et indépendante autour de mai 68 en Belgique francophone » (dir. J. Puissant)

Matières juridiques

Droit des étrangers: pratique quotidienne depuis 2002

- Droit et procédure d'asile (y compris contentieux administratif des étrangers) et droit au séjour (régularisation, regroupement familial, étudiants, détention administrative...)
- Droit sociaux des étrangers (permis de travail, aide sociale, sécurité sociale...)

Droits de l'homme et libertés fondamentales

- Droits civils et politique (vie privée, liberté d'expression...), droits économiques, sociaux et culturels (logement, aide sociale...)
- Systèmes de protection internes (contentieux judiciaire et administratif, CE et Cour constitutionnelle) et internationaux (CEDH, Pactes ONU, Charte sociale européenne, Convention internationale sur les droits de l'enfant...)

Droit de l'Union européenne

- Droit institutionnel (principes généraux, processus décisionnel, compétences...)
- Droit matériel : principes généraux de droit communautaire, 4 libertés, harmonisation en matière d'asile et d'immigration et en droit pénal...
- Contentieux communautaire (TPI et CJCE)

Droit pénal et procédure pénale; loi sur la fonction de police

Droit des obligations et des contrats (bail...)

Droit d'auteur et des médias

Droit familial (divorce, adoption, filiation)

Publications

- Nombreux articles dans *Parole à l'Exil* et *Vluchtschrift* consacrés aux droits des migrants:
<http://www.caritas-int.be/fr/publications/parole-a-lexil.html>
- « Sous les pavés, une presse libérée! Trois tentatives de journalisme radical en Belgique après 1968: «Notre Temps» (1972-1977), «Hebdo» (1975-1977) et «Pour» (1973-1982) », in J. Gotovitch, A. Morelli (ed.), *Presse communiste, presse radicale (1919-2000) Passé/présent/avenir ?*, Bruxelles, Aden, 2007, pp. 64-91.

PROCEDURES AND ACTIONS IN GERMANY, THE UK, THE NETHERLANDS AND FRANCE IN CONNECTION WITH DATABASES, LEGISLATION ON HACKERS AND DATA RETENTION

Tony Bunyan

Brief biography

Tony Bunyan is a writer and journalist and has been Director of Statewatch since 1991. He is the author of *The Political Police in Britain* (1977), *Secrecy and openness in the EU* (1999) and has edited numerous Statewatch publications including *The War on freedom and democracy – Essays in civil liberties in Europe* (2006). He has taken eight successful complaints against the Council of the European Union to the European Ombudsman on access to documents on behalf of Statewatch as well as two successful complaints against the European Commission. In 2001 and 2004 he was selected by the *European Voice* newspaper as one of the 50 most influential people in Europe.

Vanessa De Greef

Biographie sommaire

Vanessa De Greef est doctorante (FNRS) au Centre de droit public de l'Université Libre de Bruxelles. Elle est également assistante pour le cours de droits et libertés.

Elle s'est intéressée aux problématiques touchant à la vie privée et plus spécifiquement à celles touchant aux réseaux sociaux et au casier judiciaire.

Avant d'entamer sa thèse de doctorat, elle travaillait au cabinet d'avocats Progress Lawyers Network. Elle fait également partie de la Commission Justice de la Ligue des droits de l'Homme.

Verkoopprijs - Prix de vente € 15



ADVOCATEN | AVOCATS | LAWYERS

BROEDERMINSTRAAT 38 | B - 2018 ANTWERPEN | +32 (0)3 320 85 30 | +32 (0)3 366 10 75
INFO@PROGRESSLAW.NET | WWW.PROGRESSLAW.NET