# Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power[1]

**SERGE GUTWIRTH**[2]
Vrije Universiteit Brussel (Bélgica).

**PAUL DE HERT**[3]
Vrije Universiteit Brussel (Bélgica).

SUMMARY: Introduction; 1 Principles of the democratic constitutional state; 1.1 The Recognition of Human Rights in their Double Function; 1.2 The Rule of Law; 1.3 Democracy; 2 The democratic constitutional state and the invention of two complementary legal tools of power control; 2.1 Limiting power through opacity tools; 2.2 Channelling power through transparency tools; 3 Privacy as a tool for opacity (creating zones of non-interference); 3.1 The negative role of privacy; 3.2 The positive role of privacy; 3.3 The non-absolute nature of privacy; 4 Data protection as a tool for transparency; 4.1 Introduction; 4.2 The rationale behind data protection; 4.3 Data protection as an opacity tool?; 4.4 The charter of fundamental rights of the european union; 5 The shift from opacity towards transparency in european human rights law; 5.1 European human rights law and the legality requirement; 5.2 The success of the legality requirement; 5.3 A critical comment about the strasbourg focus on the legality requirement; 5.4 The danger of proceduralisation; 5.5 A requirement fundamental to opacity: necessary in a democratic state; 6. Combining privacy and data protection 6.1 Combining the tools; 6.2 Determining the switch; 6.3 An example: camera surveillance; 6.4 A second example: passenger profiling; 6.5 Workable criteria?; Conclusion.

1 Original Version available in: DE HERT P. & S. GUTWIRTH, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in E. CLAES, A. DUFF & S. GUTWIRTH (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, pp. 61-104. (ISBN 90 5095 545 2).

2 For Serge Gutwirth this contribution is partly the result of research carried out under the *Interuniversity Attraction pole* V.16 research *The loyalties of knowledge* financed by the *Belgian Federal Science Policy* (see: www.imbroglio.be).

3 For Serge Gutwirth this contribution is partly the result of research carried out under the *Interuniversity Attraction pole* V.16 research *The loyalties of knowledge* financed by the *Belgian Federal Science Policy* (see: www.imbroglio.be).

## INTRODUCTION

Privacy constitutes a relatively new concept in the development of contemporary law. Its beginnings are traditionally attributed to the famous publication of an article "The right to privacy" by the American scholars Warren and Brandeis in the *Harvard Law Review* at the end of the 19th century[4].The piece was a reaction against the state of American journalism, wherein they complained about the journalists' lack of respect for personal feelings and sexual relations. The authors called for privacy which they defined as the right to be let alone. Although notions such as secrecy and confidentiality were undeniably at the heart of the concept of privacy, there is a strong tendency in case law and literature to understand privacy as a broadly conceived concept of autonomy and information autonomy of the human person[5]. In this view, privacy embodies the freedom of choice, autonomy and self-determination of individuals in social and relational matters.

In Europe, the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), concluded in 1950, plays a crucial role regarding the protection of the right to privacy contained in Article 8 of the Convention. During the last few decades the European Court of Human Rights in Strasbourg, which has the power to make rulings about violations of art. 8 ECHR, has developed a vast and relevant but not unambiguous body of case-law about privacy.

Today, however, privacy has come increasingly under pressure, not only as a result of the large scale introduction of information technology and monitoring techniques, but also as a result of the far reaching public security policies that were devised in the aftermath of September 11. These evolutions have far reaching consequences for law enforcement. Existing principles of criminal law are challenged and traditional safeguards for defendants are threatened. In its report *Security and Privacy for the Citizen in the Post-September 11 Digital Age*, the Institute or Prospective Technological Studies (EU-Joint Research Centre) came to the conclusion that "(t)he move towards proactive surveillance reflects a transformation from the traditional legal model of gathering conclusive evidence of wrongdoing 'beyond reasonable

4 S. D. WARREN & L. D. BRANDEIS, "The right to privacy", *Harvard Law Review*, 1890, pp. 193-220.

5 E. G. S. GUTWIRTH, *Privacy and the information age*, Lanham, Rowman & Littlefield Publishers, 2002, 158 p. and Rigaux, F., *La protection de la vie privée et des autres biens de la personnalité*, Brussels/Paris, Bruylant/L.G.D.J, 1990, 849 p.

doubt' to put before a criminal court, towards an intelligence-gathering and disruptive model". This partly reflects the concerns of intelligence agencies and proactive squads to protect their information sources from disclosure to defendants in the criminal justice process, but partly a methodological shift to crime risk reduction, using probabilistic profiles to stop criminals (especially terrorists) from reaching their targets, concluding business deals or purchasing businesses/property to integrate into the upper world. This then raises important questions for the preparedness of the criminal justice systems of Member States and court-oriented protections for citizens. "What will the role of the courts be, and how will the use of secret intelligence to guide police actions be treated for disclosure to defendants to protect their rights?"[6].

These findings and questions are essential for our present study of privacy and criminal procedure. The evoked shifts in policing strategies have been opposed by civil rights movements and legal authorities precisely with privacy arguments. The tone of the debate has often been rather dark, with many doom scenario's and catchphrases such as *The Death of Privacy* or *The End of Privacy...*

We believe that there is no reason why these scenarios should become an European reality. Europe has a long, stable tradition of dealing with power demands and threats to human rights. To discover this tradition we first look into the constitutional role that privacy plays in our liberal democratic constitutional state, thereby distinguishing between privacy and data protection. For us privacy is an example of a "tool of opacity" (stopping power, setting normative limits to power), while data protection and criminal procedure can be mainly – not exclusively – seen as "tools of transparency" (regulating and channelling necessary/reasonable/legitimate power). Much can thus be learned from making and ascertaining the differences in scope, rationale and logic between privacy on the one hand, and data protection on the other. This is, in two short sentences, both the program and the challenge of this contribution.

New threats to privacy should and can be addressed by using measures relating to privacy *and* data protection. Examples such as video surveillance

6 Institute For Prospective Technological Studies – Joint Research Centre, "*Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*. *Report to the European Parliament Committee on Citizens" Freedoms and Rights, Justice and Homme Affairs* (LIBE), July 2003, IPTSTechnical Report Series, EUR 20823 EN, 97 (our emphasis). See also: ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.

and data gathering by the U.S. Department of Homeland Security (CAPPS-II) show how privacy and data protection have their respective and different roles to play. We critically assess the case-law of the European Court of Human Rights. In its current formulation, the privacy doctrine by the European Court neglects the importance of opacity in a democratic state. The European judges prefer to focus on much safer issues such as accountability and foreseeability, whereas our times are in need of more or less clear-cut statements about the reasonableness of new police powers that are developed within and outside Europe.

## 1 PRINCIPLES OF THE DEMOCRATIC CONSTITUTIONAL STATE

The project of the democratic constitutional state has engendered alternative ways of dealing with power and brought about a specific concept of the state in which power is by definition limited. The aims of the democratic constitutional state are generally translated, expressed and concretised through the enactment of three basic constitutional principles, namely the recognition of fundamental rights and liberties, the rule of law (constitutionalism) and democracy. These three principles will be briefly discussed hereafter[7].

### 1.1 The recognition of human rights in their double function

First, the constitutions of democratic constitutional states recognise a set of individual fundamental rights and freedoms (or shortly: human rights) that are deemed to be at the very core of the political construct[8].

7 This chapter includes parts of P. DE HERT & S. GUTWIRTH, "Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence" in Institute For Prospective Technological Studies – Joint Research Centre, *o.c.*, pp. 111-162. Available at: ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf. See also S. GUTWIRTH, "De polyfonie van de democratische rechtsstaat" [The polyphony of the democratic constitutional state] in *Wantrouwen en onbehagen*, M. ELCHARDUS (editor), Balans 14, Brussels, VUBPress, 1998, pp. 137-193.

8 According to the original political philosophy of the Enlightenment (Locke, Rousseau, [...]) these rights are *natural rights*. This view sees individuals as the holders of inalienable rights because of the mere fact that they are humans. This implies that the individual exists as the bearer of a number of eternal and universal rights which transcend and bind the (temporal) power of the state. One step further, it is argued that if a government, does not respect these rights, it becomes illegitimate and the people have the right to resist and to abolish it (cf. LOCKE, the *Declaration of Independence* and the *Déclaration des droits de l'homme*). We are not willing to enter the debate about the theory of natural rights. Elsewhere, however, and inspired by Rawls, we defend a non-comprehensive and non-essentialist, but political and constructivist (pragmatic) approach on human rights and basic liberties; cf. P. DE HERT & S. GUTWIRTH, "Rawls" political conception of rights and liberties. An unliberal but pragmatic approach to the problems of harmonisation and globalisation" in M. VAN HOECKE (Editor) *Epistemology and Methodology of Comparative Law*, Hart Publications, Oxford/Portland, 2004, pp. 317-357.

In principle, the State is not allowed to encroach upon or to interfere with these rights. Human rights work as a shield or a bulwark. They express the recognition of the power of the individual, drawing the limits and frontiers of the power of the state and of state intervention[9]. Hence, individuals have acquired a package of elementary prerogatives against the state power[10]. For the understanding of privacy and its implications, it is crucial to bear in mind that this recognition of human rights affirms the existence of the human individual as an independent being, detached from the state but also from the politics driven by a democratically elected majority. Human rights protect individuals against J. S. Mill's proverbial "tyranny of the majority". In other words, they create a sphere of individual autonomy or self-determination and in doing so, they protect individuals against excessive steering of their lives; they contribute to the creation of the private sphere[11].

Human rights and liberties not only restrict the power of the state, but also empower citizens (or individuals) to participate in the political system[12]. This second important function of human rights explains why within the Western political tradition, it may not be too hard to find an overlapping consensus on the importance of basic liberties, such as freedom of expression, liberty of conscience and freedom of association. These rights and liberties enable citizens to develop and exercise their moral powers in forming, revising and in rationally pursuing their conceptions of the good[13].

---

9 This is easy to understand as the revolutionary people of the 17/18th century in England (1688 Bill of Rights), the USA (1776 Declaration of Independence and 1788-1791 *US Constitution*) and France (1789 *Déclaration*), which laid the building stones of the democratic constitutional state, were simultaneously doing two things. On the one hand, they did put an end to the arbitrary and absolute power of the former sovereigns and, as such, the described (r)evolutions can be said to have broken with the political economy of the past. On the other hand the actors of the three (r)evolutions laid the basis for a new constitutional system in order not only to make absolutism and arbitrary power relations impossible in the future but also to build up a new kind of society wherein individual liberty and entrepreneurship would prevail.

10 Actually this is also, but indirectly, the case pertaining to the power of other societal actors.

11 Of course, it must be said that this sphere of autonomy and self-determination is not an absolute one: it is subject to limitation, through legal mediation processes of legislative and/or judicial nature, in name of the protection of the rights and interests of the other citizens or of the public interest. This is indeed the case of privacy, which, beyond the fact that it is an quintessential value in a democratic constitutional state, is nonetheless not offering an absolute protection to its holder (cf. *infra*).

12 C. SCHNEIDER, "The Constitutional Protection of Rights in Dworkin's and Habermas 'Theories of Democracy'", *UCL Jurisprudence Review*, 2000, 118 with reference to Charles Larmore ("The Foundations of Modern Democracy: Some Remarks on Dworkin and Habermas", *European Journal of Philosophy*, 1995, 65) who has observed that "individual rights serve, not to protect us against the collective will, but rather to protect the means necessary for creating a collective will". Cf. P. DE HERT & S. GUTWIRTH, "'Rawls' Political Conception of Rights and Liberties", *l.c.*, pp. 317-357.

13 J. RAWLS, *Justice as Fairness. A Restatement*, Cambridge, Harvard UP, 2001, § 13.4.

### 1.2 The rule of law

Secondly, the constitutions of democratic constitutional states all enshrine the rule of law and constitute a *Rechtsstaat*. The constitutional recognition and implementation of the rule of law again tend to limit the power of government, but this time this happens no longer through setting a limit to the reach of the power, but through what one could call a system of "internal" organisation of government and power. Nonetheless, the objective remains the same, namely the protection of individuals against excessive and arbitrary domination. The main idea of the rule of law is the subjection of government and other state powers to a set of restricting constitutional rules and mechanisms[14].

On the one hand the rule of law provides for the principle of legality of government, which stands for the basic principle that power can only be exercised in accordance to the law. From this perspective public authorities are bound by their own rules and can only exercise their powers in a lawful way. All powers must derive from the constitution (which in its turn is deemed to translate the will of the sovereign people) and any exercise of power must be interpretable as emanating from a constitutional provision. This implies the important fact that the government is accountable and that its actions must be controllable, and thus transparent. "The rule of law" thus refers to the idea that our societies are governed by rational and impersonal laws and not by the arbitrary commands of humans. Moreover, because these laws must be general and apply to all, they (at least formally) embody the principle of equal treatment and protection of the laws[15].

On the other hand the rule of law establishes the trias politica or, in other words, a system of balancing of powers. Here the basic idea is to limit the power of the state by spreading it over different centres, with different competencies and functions. These powers – the executive, legislative and judicial power – are constitutionally doomed to work together through a dynamic system of mutual control or checks and balances. This system relies heavily on the famous ideas which Montesquieu developed in *De l'esprit des lois*: "Pour qu' on ne puisse abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir"[16]. Indeed, the best way to limit

14 J. CHEVALLIER, *L'Etat de droit*, Paris, Montchrestien, 1994, p. 11.
15 K. RAES, *Tegen betere wetten in. Een ethische kijk op het recht*, Gent Academia Press, 1997, p. 215.
16 MONTESQUIEU, *De l'esprit des lois*, t. 1, Paris, Garnier-Flammarion, 1979, p. 293.

power is to divide it up and to spread it over competing centres. In sum: the trias politica replaces a centralist power by a pluricentric power economy[17]. Such a system implies the mutual accountability of state powers, and thus again, the reciprocal transparency and controllability of the legislative, the judicial and, last but not least, the executive power.

### 1.3 Democracy

Thirdly, the constitutions of democratic constitutional states recognise the postulate of the people's sovereignty and the principles of democracy and democratic representation. During the political Enlightenment the sovereignty of the rulers gave way to the people's sovereignty and the idea of the political self-determination of the nation. Consequently, in a democratic constitutional state the only valid justification of power must be sought in the citizens' consent or will. This crucial link is expressed through the different variations upon the theme of the social contract (Beccaria, Locke, Rousseau [...]), for such contracts construe the constitution of a political entity with reference to the will or consent of the individuals. State powers are derived from the sovereignty of the citizens.

More concretely, these theoretical foundations of state power imply that government in all its aspects must be in line with the public or general interest and must mainly be driven by the will of the majority. Hence, systems of representation and participation of citizens are of crucial importance. State organs and institutions must be representative. Participation by citizens in political decision-making must be organised and stimulated. And, last but not least, systems of democratic governance must provide procedures for the direct and indirect control of the public authorities by the citizens. As a result democratic rule implies the accountability of the government towards the citizens, which again calls for transparency of public decision-making and policies.

The foregoing analysis can be summarised by highlighting the fact that the development of the democratic constitutional state has led to the invention and elaboration of two complementary sorts of legal tools which

17 R. FOQUE, "Rechtsstatelijke evenwichten in de trias politica. De actuele betekenis van de onafhankelijkheid van de rechterlijke macht", *Vigiles – Tijdschrift voor politierecht*, 1996/4, pp. 1-5 and R. FOQUE, "Rechtsstatelijke vernieuwing. Een rechtsfilosofisch essay" in P. KUYPERS, R. FOQUE & P. FRISSEN, *De lege plek van de macht. Over bestuurlijke vernieuwing en de veranderende rol van de politiek*, Amsterdam, De balie, 1993, pp. 18-44.

both aim at the same end, namely the control and limitation of power. We make a distinction between on the one hand tools that tend to guarantee non-interference in individual matters, or the opacity of the individual, and on the other, tools that tend to guarantee the transparency/accountability of the powerful[18]. This will enable us, in the following sections, to link privacy to the first tool and data protection to the second.

## 2 THE DEMOCRATIC CONSTITUTIONAL STATE AND THE INVENTION OF TWO COMPLEMENTARY LEGAL TOOLS OF POWER CONTROL

### 2.1 Limiting power through opacity tools

As the core aim of a democratic constitutional state is to foster an order driven by individual liberty, the protection of individuals against state interference is at premium. Hence, the importance of the private sphere as a sphere where individual liberty has a privileged status cannot be underestimated. That is why opacity tools that shield individuals against state interference are so crucial.

The ideas behind such tools can be understood by recalling the function of the first generation of human rights. By recognising human rights, the revolutions of the 17th-18th centuries in England, the US and France laid the foundations for a sharper legal separation between the public and private spheres[19]. The constitutional recognition of these rights led to the creation of a sphere of individual autonomy and self-determination, where the citizens may live their lives without interference of the state. Human rights have empowered the individuals through recognition of their liberty and prerogatives. And inversely, limits to state power were drawn through the recognition of the autonomy of the citizens.

Thus, human rights can be understood as legal tools that protect individuals against interference by the state and by private actors. They tend to require abstention from undesired intervention in matters that are essential for the protection of the individual's autonomy and liberty.

18 "Opacity" designates a zone of non-interference which in our opinion must not be confused with a zone of invisibility: privacy for instance does not imply secrecy, it implies the possibility of being oneself openly without interference. Another word might have been "impermeability" which is too strong and does not contrast so nicely with "transparency" as "opacity" does.

19 See Ph. ARIES & G. DUBY G. (editors), *Histoire de la vie privée* and particularly M. Perrot (editor), *Volume 4: De la Révolution à la Grande Guerre,* Paris, Le Seuil, 1987, p. 637.

A good example is the protection of the "sanctity" or inviolability of the home, which indeed properly expresses the concern for respect for individual autonomy: public authorities (but also other citizens) must respect the bounds of the home. A home is inviolable, and any breach of that principle generally engenders criminal prosecution. Once inside their home, people are more free from interference from the government (and others) than they are outside. A home is a privileged setting. Within a home, each and every person has the freedom to do as he/she pleases, uninhibited by society's social and ethical mores. U.S. case law has already shown, *e.g.*, that watching pornography at home and possessing obscene movies, which may not be distributed in public, is protected by the inviolability of the home. Providing home entertainment by serving food naked cannot be outlawed in the same way than such entertainment in bars and restaurants is. This does not mean that everything happening inside the home is automatically protected. Search warrants can be ordered in criminal cases, but only, in principle, if a series of stringent conditions are met[20]. Crimes and unlawful acts are not condoned because they happen to take place within a home. But because a home is granted a special measure of protection, trespassing by third parties and especially by the police and judicial authorities is strictly regulated.

The relationship between opacity tools and individual liberty is far from simple. The latter is undeniably the prime concern of the former, but the relationship is not without ambiguity, for opacity tools supersede individual consent when societal interests are at stake[21]. What is essential to opacity

20 The political function of the right to have the house protected and the idea that limitations are still possible, have been recognised by the European Court in the *Niemietz* judgement: "More generally, to interpret the words 'private life' and 'home' as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8 (art. 8), namely to protect the individual against arbitrary interference by the public authorities (see for example: *Marckx v. Belgium*, judgement of 13 June 1979, § 31). Such an interpretation would not unduly hamper the Contracting States, for they would retain their entitlement to 'interfere' to the extent permitted by paragraph 2 of Article 8 (art. 8-2); that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case"; *Niemietz v. Germany*, judgement of 16 December 1992, § 32). *Note about our references to the judgements of the European Court of Human Rights*: in a first reference to such a judgement we will mention the name of the applicant and the respondent state, as well as the date of the judgement. With these data the judgements can easily be found at: http://www.dhcour.coe.fr/eng/. After the first reference that we will only use the name of the applicant (ex. *Niemietz*). For precise references and quotes we will refer to the relevant paragraphs of the judgements.

21 A fine example is found in the provisions in the Directive no. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal of the European Communities*, L 281, 23 November 1995, 31-50 (further cited as Data Protection Directive) establishing a public law regime that cannot be varied by a private law contract. Consequently, any agreement pursuant to which a data subject waives some or all of his rights under the Data Protection Directive is void and unenforceable, even if the agreement otherwise meets

tools is their normative nature. Through these tools, the (constitutional) legislator takes the place of the individual as the prime arbiter of desirable or undesirable acts that infringe on liberty. This collective, normative dimension of opacity tools explains the complex relationship between human rights and individual liberty. The harm principle as a yard stick to measure wrongful infringements on individual liberty is replaced by a more formal criterion[22], and ad hoc balancing is replaced by categorical balancing[23]. The stated goal of human rights, even in cases when they limit freedom by taking away consent, is the protection of individual liberty. Through the implementation of these tools, the outcome of conflicts becomes more predictable: the balancing of (conflicting) interests has already been done in favour and in the name of the subject. One author holds that "a right defining liberty often offers greater protection than the liberty itself"[24].

It is however evident that categorical balancing does not always result in the greatest possible protection of the individual, for instance when (constitutional) texts provide for intrusions into the home when a search warrant has been obtained. Therefore, it is more precise to emphasise the normative rather than the protective function of opacity tools. Through such tools the (constitutional) legislator enacts hard or clear norms. Choices about the way liberty interests and other interests should be balanced are made in an abstract way. Complexity is reduced. Of course, complexity can be reduced to the full detriment of liberty, but since this would go against the spirit of the Western constitutional state as defined above, this may not be taken seriously as a hypothesis.

To end this section, we wish to underline that opacity tools do not necessarily take the form of a human rights provision enshrined in an international treaty or national constitution. For instance the existence and intervention of the investigating judge in the criminal process is a good example of an opacity tool, because it expresses a clear or hard choice to grant special status to the protection of the private sphere. However, in common law legal systems there is no such institution. And even the

all validity requirements and is in the data subject's interest. Although data protection, when applied, will be identified as a typical transparency tool (*infra*), it is constructed on public law foundations. The sheer existence of European data protection law in its present (public law) form is a "hard" choice.

22 J. Ravanas, annotation to Cour de Cassation (Fr.), 5 March 1997, *Recueil Dalloz*, (Cahier Jurisprudence), 1998, v. 34, (474-476), 475 with reference to the work of François Rigaux: "La sanction est fondée sur la violation du droit de demandeur, quel que soit le comportement du défendeur".

23 *Ibid.*

24 *Ibid.*: "Que la liberté devienne un droit, la protection en sort renforcée".

constitutions of Continental legal systems (Belgium, the Netherlands, [...]) are silent about the investigative judge, although his position in the criminal process is central. There is properly speaking no human right to have a criminal investigation done by an investigative judge, but there is a legal set of rules that recognises such a positive right[25].

### 2.2 Channelling power through transparency tools

The second set of tools is connected to the principles of the democratic constitutional state that limit the state powers, not by drawing the limits of their reach through the recognition of a private sphere of autonomy, but by devising legal means of control of these powers by the people, by controlling bodies or organisations and by the other state powers. These tools have the common feature that they are intended to compel government and private actors to "good practices" by focusing on the transparency of governmental or private decision-making and action, which is indeed the primary condition for an accountable and responsible form of governance. The system of checks and balances, for example, installs the mutual transparency of state powers, while the controllability and accountability of government by the citizens implies free and easy access to readily available government information, the enactment of swift control and participation procedures, the creation of specialised and independent bodies to control and check the doings of government, and so on.

The tools of opacity are quite different in nature from the tools of transparency. Opacity tools embody normative choices about the limits of power; transparency tools come into play after these normative choices have been made in order still to channel the normatively accepted exercise of power. While the latter are thus directed towards the control and channelling of legitimate uses of power, the former are protecting the citizens against illegitimate and excessive uses of power. The latter do take into account that the temptations of abuse of power are huge, and empower the citizens and special watchdogs to have an eye even on the legitimate use of power: they put counter powers into place. The former determine what is in principle out of bounds for governmental and private actors and, hence, what is deemed so essentially individual that it must be shielded against public and private

25 P. DE HERT, "Het recht op een onderzoeksrechter in Belgisch en Europees perspectief. Grondrechtelijke armoede met een inquisitoriale achtergrond" [The investigating judge in Belgian and European Law], *Panopticon. Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, 2003, pp. 155-198.

interference. On the one hand there is a regulated acceptance; on the other there is a prohibition rule, which is generally subject to exceptions[26].

This second set of tools is particularly useful for regulating relationships between private actors. As a starting point for such relationships it should be accepted that these actors have equal claims to liberty and are in principle capable of protecting their own liberty interests. Individual consent and ad hoc balancing are suitable instruments to reconcile the liberty interests at stake. Only after careful consideration and with solid arguments, for instance with regard to unequal power relationships, should governments interfere and impose "hard norms" or "choices" resulting from categorical balancing.

## 3 PRIVACY AS A TOOL FOR OPACITY (CREATING ZONES OF NON-INTERFERENCE)

### 3.1 The negative role of privacy

Privacy pre-eminently imposes itself as the legal concept translating the political endeavour to ensure non-interference (or opacity) in individual matters. It is embedded in the contemporary democratic constitutional state, the values of individualism and the constitutional separation between state and church. It is also intimately linked with the idea that individuals are able and willing to unshackle themselves from tradition, social conventions or religion and dissociate themselves, up to a point, from their roots and upbringing. Privacy, negatively stated, protects individuals against interference in their autonomy by governments and by private actors[27]. It is a fundamental notion for a project of society that wants to limit power relationships.

The work of the French liberal Benjamin Constant (1767-1830) is illustrative and very important in this respect[28]. Constant can claim

26 In essence the second category of tools overlaps with administrative law promoting and ensuring accountability by governmental actors. Its logic can also be found in Western labour law. Without touching the power relations between workers and employers, this set of rules provides for a kind of procedural justice, viz. rules to be followed when taking certain decisions that cannot be challenged due to differences in power position, but that can be checked for fairness in the decision making.

27 Such a negative understanding of privacy can clearly be read in the formulation of Article 8 ECHR: no interference by public authorities is permitted unless necessary in a democratic society.

28 In particular *Principes de politique*, written between 1806 and 1810 but first fully published in1980: B. CONSTANT, *Principes de politique applicable à tous les gouvernements*, (1806-1810), E. HOFMANN (editor), Hachette, Paris, 1997, p. 447. See on Constant: P. DE HERT, "The Case of Anonymity in Western Political Philosophy. Benjamin Constant's Refutation of Republican and Utilitarian Arguments against Anonymity", in C. NICOLL, J. E. J. PRINS & M. J. M. VAN DELLEN (editors), *Digital Anonymity and the Law.*

fatherhood, not only of the paradigm of the state as a potential menace to individual liberty, but also of terms such as "liberalism", "private life" ("vie privée"), "surveillance", "individual liberty" and "the individual" so dear to modern privacy thinking. Constant saw the recognition of privacy and individual liberty as an unavoidable fact and coupled this from the start to the idea of limited government. This liberal militancy was born out of the spirit of doubt. He was convinced that no group of mortals could be certain about the nature of virtue or the human good and he was ready to oppose any regime that claimed such certainty[29]. No social telos could be so unquestionable as to justify legal enforcement. Governmental attempts to outlaw dissent, legislate public morality, and inculcate civic virtue are paternalistic violations of the purity of man's moral judgement and his capacity to seek for the truth himself[30]. Individuals lose their critical attitude once the truth is imposed upon them. States should limit themselves to their primary task; they should abolish all moral institutions and preserve only the necessary political institutions. Individual liberty should be surrounded with institutional arrangements that keep open and accessible a wide variety of social and political possibilities. Modern times, Constant holds, create a desire for privacy in us (we "must" turn towards the freedom "of peaceful enjoyment and private independence"). Everything that supposes the unnecessary submission of the individual to society should be redefined in the name of individual liberty by applying the harm principle: criminal laws, sexual and religious codes, mores, taxes, state regulation of commerce and industry, state propaganda and access to the media, public schools, army recruitment, etc.

### 3.2 The positive role of privacy

Privacy also functions positively. Being the legal concept that embodies individual freedom, it plays a quintessential role in the democratic constitutional state based upon the idea that its legitimacy can only result from a maximal respect of each person's individual liberty. Privacy protects the fundamental political value of a democratic constitutional state as it

*Tensions and Dimensio*, Volume 2 Information Technology & Law Series (IT&Law Series), The Hague, TMC Asser Press, 2003, pp. 47-97.

29 S. HOLMES, *Benjamin Constant and the Making of Modern Liberalism*, New Haven, Yale University Press, 1984, 7.

30 B. CONSTANT, *o.c.*, Book XIV, Chapter III, 313-314; Chapter V, 317. On Constant's defense of self-interest against paternalism, see S. HOLMES, *o.c.*, pp. 252-254.

guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards – for example – their sexuality, health, personality building, social appearance and behaviour, and so on. It guarantees each person's uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests or with the public interest[31].

In literature the close bond between the negative and positive functions of the right to privacy and its necessity for political life have been rightly stressed. Within Arendt's[32] and Habermas's[33] construction of the public sphere, a space for individuals is provided to develop their own identity and ideas in order to engage in public life. The ideal of a "public" government necessarily entails its opposite: a "private" sphere, protected from public intervention, within which people are free to form individualised relationships that cannot be justified under the requirements of impersonal beneficence[34].

This view is echoed in the available privacy literature[35] and in many anthropological studies. These studies have made it clear that observation

31 About this concept of privacy see a.o. S. GUTWIRTH, *Privacy and the information age*, *o.c.*, *passim* and S. GUTWIRTH "Privacyvrijheid" een voorwaarde voor maatschappelijke diversiteit" [Privacy's freedom: a condition for social diversity] in *Eenheid en verscheidenheid in recht en rechtswetenschap*, A. M. P. GAAKEER & M. A. LOTH (Red), *SI-EUR Reeks 28*, Arnhem, Kluwer/Gouda Quint, 2002, pp. 95-138.

32 Arendt speaks of "the danger to human existence from the elimination of the private realm"; H. Arendt, *The Human Condition.* Chicago: University of Chicago Press, (1958), 1998, 70. She further notes that there are "a great many things which cannot withstand the implacable bright light of the constant presence of others on the public scene", for example, love, and that "a life spent entirely in public, in the presence of others, becomes [...] shallow" (*ibid.*, 71). Arendt therefore recognises that without a private space for identity formation and the shielding of intimate details from others, the public could never be constituted. Indeed she concludes that public and private can "exist only in the form of coexistence" (*ibid.*, p. 59).

33 Compared to Arendt, public sphere theorist Jürgen Habermas carves out a similar yet more powerful role for the private sphere. For Habermas, more than simply coexistent, the private sphere literally constitutes the public. "The bourgeois public sphere may be conceived above all as the sphere of private people who have come together as a public"; J. HABERMAS, *The Structural transformation of the public sphere.* Translated by Thomas Berger and Frederick Lawrence. Cambridge, Mass., MIT Press., 1989, p. 26.

34 L.M. SEIDMAN, "Public Principle and Private Choice", *Yale Law Journal,* Volume 96, 1987, p. 1026.

35 On the positions taken by privacy authors such as Diffie and Landau, Reiman and Bloustein, see Ch. HUNTER, "Political privacy and online politics: how e-campaigning threatens voters privacy", *First Monday,* v. 7, no. 2, (February 2002), 4. Interesting in the light of the Kantian position is the point made by Bloustein: "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual"; E. J. BLOUSTEIN, "Privacy as an Aspect of Human Dignity", in F. D. SCHOEMAN (editor), *Philosophical Dimensions of Privacy: An Anthology,* New York, Cambridge University Press, 1984, 188. Both Kant and Bloustein ground their argument of the notion of human dignity, with very different outcomes.

by listening or watching which is known to the subject necessarily exercises a restrictive and/or steering influence over him: he must either bring his actions within the accepted social norms in the particular situation involved or decide to violate those norms and accept the risk of reprisal[36].

The significant role of privacy, instrumental to the building of the citizen, should also be understood in the light of Michel Foucault's that all power relationships presuppose a tension between the power and the individual resistance it appeals to. Power as a behavioural conduit – *une conduite des conduites* – always implies a moment of resistance, namely the moment when individuals consider behavioural alternatives. Foucault sees power as the relation between individuals, when one steers the behaviour of the other, even though the other has the freedom to act differently. Power in this sense is a strategic situation that leads individuals to behave in ways to which they would not spontaneously commit themselves[37]. Resistance, Foucault writes, is always at the heart of the balance of power. And it is precisely at this elementary level that privacy comes in, since personal freedom embodies behavioural alternatives other than those induced by the power relation. In other words, privacy is the legal recognition of the resistance or reticence to behaviour steered or induced by power. From this point of view, privacy in a constitutional democratic state represents a legal weapon against the development of absolute balances of power, again proving privacy's essential role in such a state[38].

---

36 On the work of Robert Merton and others, see A. WESTIN, *Privacy and freedom*, London, The Bodley Head Ltd, 1970, 13 and 58. One could easily argue that persons who have not committed criminal acts should not fear being surveilled, but this argument is based on the erroneous assumption that a society or a group should or can function on the basis of the full observability of its members. The individual in virtually every society engages in this continuing process of what could be called *social distance setting*. It is one of the key universal dialectical processes in social life. The reason for the universality of this process is precisely that individuals have conflicting roles to play in any society. A certain degree observation will prevent members of the group from performing effectively. Some measure of leeway in conforming to role expectations is presupposed in all groups and makes social life possible. To have to meet the strict requirements of a role at all times, without some degree of deviation, is to experience insufficient allowances for individual differences in capacity and training and for situational exigencies which make strict conformity extremely difficult. The surveillance also constrains the observer, since he must decide whether or not to act against the non-complying person and must measure the effects of not acting on the group perception of authority.

37 Cf. M. FOUCAULT, "Deux essais sur le sujet et le pouvoir" in H. DREYFUS & P. RABINOW, *Michel Foucault. Un parcours philosophique*, Paris, Gallimard, 1984, 313-314: "L'exercice du pouvoir [...] est un ensemble d'actions sur des actions possibles: il opère sur le champ de possibilités où vient s'inscrire le comportement de sujets agissants: il incite, il induit, il facilite ou rend plus difficile, il élargit ou limite, il rend plus ou moins probable; à la limite il contraint ou empêche absolument; mais il est bien toujours une manière d'agir sur un ou sur des sujets agissants, et ce tant qu'ils agissent ou qu'ils sont susceptibles d'agir. Une action sur des actions".

38 So privacy imposes a balancing of power and resistance in all power relationships. And this does – or at least should – not only apply to the interference of the state. The list also includes the business sector, companies, trade unions, police, doctors, etc. The legal system gives examples – some successful, some not – of attempts

### 3.3 The non-absolute nature of privacy

Before going any further it is necessary to recall that affirming the essential role of privacy does not at all imply that privacy and the freedom it protects are absolute or inviolable values. On the contrary, notwithstanding privacy's core importance in a democratic constitutional state it is clear that it is a relatively weak fundamental right[39]. Actually, not a single aspect of privacy takes absolute precedence over other rights and interests. That includes confidentiality of the mail, physical integrity and control over personal information. Never does an individual have absolute control over an aspect of his/her privacy. If individuals do have the freedom to organise life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that stage, the rights, freedoms and interests of others, as well as the prerogatives of the authorities, come into play. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance. This shows clearly that, although quintessential for a democratic constitutional state, because it refers to liberty, privacy is a relational, contextual and per se social notion which only acquires substance when it clashes with other private or public interests[40].

In general, the legal profession does not like to work with absolute values[41]. Of particular relevance to the privacy right is the republican argument against complete privacy. For the republican school absolute privacy may be detrimental to the building of citizenship. Rousseau, a classic example of the republican stand, stresses the need for the citizen to

to safeguard the privacy of individuals by protecting it against powerful interests. Police services cannot invade the privacy of a home at will. Welfare workers also have to operate within limits. Homeowners do not have the unlimited right, despite the absolute right to property, to check on their tenants. Employers cannot check on their personnel and their telecommunication exchanges at will. Banks and insurance companies are, in principle, limited in their freedom to gather, process and pass on personal information.

39 This is nicely illustrated by the fact that the ECHR *e.g.* recognises different sorts of human rights. The ECHR recognises some so called "hard core" or absolute rights that must be respected even in times of emergency when derogations to other rights are justified (art. 15 § 2 ECHR). Next to this there are "normal rights" (*e.g.* art. 5 and 6 ECHR) which can be derogated from in times of emergency (art. 15 § 1). Finally the ECHR counts four rights which can be legitimately restricted in terms of emergency but also under some specified conditions (art. 8-11 ECHR, the conditions for permissible restrictions are listed in the second paragraphs of these Articles). Privacy is one of these "restrictable rights".

40 In these cases (and on a case by case basis) it will be up to the legislator or the judge to determine how heavily privacy weighs against other rights and legitimate interests. But if privacy is found to prevail in a case, this will lead to a prohibition of interference.

41 C.R. SUNSTEIN, *Legal Reasoning and Political Conflict*, Oxford, O.U.P., 1996, p. 220.

participate in the public sphere to achieve "true freedom"[42], and warns that private concerns threaten the functioning of good government. The rise of self-interest would mean the end of the state[43]. A contemporary preference for public political engagement and suspicion of private action, is found in the work of Nancy Fraser. Her civic republicanism sees politics as people reasoning together to promote a common good that transcends the mere sum of individual preferences. The idea is that through deliberation members of the public can come to discover or create such a common good. In the process of their deliberations, participants are transformed from a collection of self-seeking, private individuals into a public-spirited collectivity, capable of acting together in the common interest. On this view, private interests have no proper place in the political public sphere[44]. Other contemporary defences of the virtues of public life are contained in Jürgen Habermas's *The Structural Transformation of the Public Sphere*[45] and Hannah Arendt's *The Human Condition*. Both authors were quoted above when discussing the need for privacy and opacity in a democratic state. However, both political thinkers are careful not to overestimate the importance of privacy. Relying heavily on Greek and Roman concepts, Arendt argues that, for people to be truly human, they need to live a more public life. For Arendt, politics is the vita activa or active life, where "human life in so far as it is actively engaged in doing something, is always rooted in a world of men and of manmade things which it never leaves or altogether transcends"[46]. She complains that the modern concept of privacy as sheltering us from social and political life is harmful as it does not allow us to become full humans, which can only

42 He holds that man acquires, together with civil society, moral freedom, which alone makes man the master of himself, "for to be governed by appetite alone is slavery, while obedience to a law one prescribes oneself is freedom". Cf. J. J. ROUSSEAU, *Du contrat social* (1762) in *Oeuvres complètes de Jean-Jaqcues Rousseau*, edited by B. GAGNEBIN and M. RAYMOND, Paris, Gallimard (Pléiade), 1964, Book 1, Chapter VIII, p. 365.

43 "As soon as public service ceases to be the chief business of the citizens and they would rather serve with their money than with their persons, the State is not far from its fall. [...] The better the constitution of a State is, the more do public affairs encroach on private in the minds of the citizens. Private affairs are even of much less importance, because the aggregate of the common happiness furnishes a greater proportion of that of each individual, so that there is less for him to seek in particular cares. In a well-ordered city every man flies to the assemblies; under a bad government no one cares to stir a step to get to them, because no one is interested in what happens there, because it is foreseen that the 'general will' will not prevail, and lastly because domestic cares are all-absorbing. Good laws lead to the making of better ones; bad ones bring about worse. As soon as any man says of the affairs of the State, 'What does it matter to me?', the State may be given up for lost"; J. J. ROUSSEAU, *o.c.*, Book 3, Chapter XV, p. 429.

44 N. FRASER, "Rethinking the Public Sphere" in C. CALHOUN (editor), *Habermas and the Public Sphere*, Cambridge Mass., MIT Press, 1992, 130; Ch. Hunter, *l.c.*, p. 3.

45 J. HABERMAS, *The Structural transformation of the public sphere.* Translated by Thomas Berger and Frederick Lawrence. Cambridge, Mass.: MIT Press., 1989.

46 H. ARENDT, *The Human Condition.* Chicago: University of Chicago Press, (1958), 1998, p. 22.

occur through engaging in an active public life with other people. "To live an entirely private life means above all to be deprived of things essential to a truly human life"[47]. Arendt comments that even the most intensely private actions cannot be fully understood until they are made public to others[48].

Opacity can also hide immoral and illegal actions. It can therefore be strongly argued that an ideal open society might be best served by total mutual transparency of all actors, as David Brin, treading in republican footsteps, contends[49]. However, there can exist good reasons and contexts to favour the elaboration of prohibitionary privacy/opacity rules, of which a number already do exist. They translate the need to shelter individuals against a too intrusive *conduite de la conduite* by more powerful social actors.

## 4 DATA PROTECTION AS A TOOL FOR TRANSPARENCY

### 4.1 Introduction

Since the 1970s, several European states have passed data protection legislation, that is, legislation protecting individuals from abuse resulting from the processing (i.e., the collection, use, storage, etc.) of personal data by public administrations and private actors. In general, these laws specify a series of rights for individuals and demand good data management practices on the part of the entities that process data ("data controllers"). The starting point of data protection is the desire to protect the citizen. Its purpose is to ensure that personal data are processed in ways that make it unlikely that personal integrity and privacy will be infringed or invaded[50].

It is impossible to summarise data protection in two or three lines. "Data protection" is a catch all term for a series of ideas with regard to the processing of personal data (cf. infra). Through the application of these ideas governments try to reconcile fundamental but conflicting values such

47 *Ibid.,* p. 58.

48 "Compared with the reality which comes from being seen and heard, even the greatest force of intimate life – the passions of the heart, the thoughts of the mind, the delights of the senses – lead an uncertain, shadowy kind of existence unless and until they are transformed, deprivatised and deindividualised, as it were, into a shape to fit them for public appearance" (*Ibid.,* 50).

49 D. BRIN, *The transparent society. Will technology force us to choose between privacy and freedom*, Perseus publ., 1999, p. 378.

50 P. BLUME, "The Citizens" Data Protection", *The Journal of Information, Law and Technology*, 1998/1 http://elj.warwick.ac.uk/jilt/infosoc/98_1blum/ (9p.), pp. 1-2.

as privacy, free flow of information, governmental need for surveillance and taxation, etc. In general data protection does not have the prohibitive nature of criminal law. The data subject does not own his data and he or she cannot in many cases prevent processing of his data. Under the current state of affairs, data controllers are recognised to have a right to process data pertaining to others. Hence, data protection is pragmatic in nature: it assumes that private and public actors need to be able to use personal information and that this in many cases must be accepted for societal reasons. The "thou shall not kill" that we know from criminal law, is replaced by a totally different message: "thou can process personal data under certain circumstances". The principled rupture in logic is evident.

### 4.2 The rationale behind data protection

Data protection is not prohibitive. On the contrary, in the public sphere, it is almost a natural presumption that public authorities can process personal data as this is necessary for the tasks they have to perform under statute, since, in principle, public authorities in democratic societies act on behalf of the citizens. The main aims of data protection consist in providing various specific procedural safeguards to protect individuals' privacy and in promoting accountability by government and private record-holders. Data protection laws were precisely enacted not to prohibit, but to channel power, viz. to promote meaningful public accountability, and provide data subjects with an opportunity to contest inaccurate or abusive record holding practices. The rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems there is an urge to collect, store and use data, an urge which must be curtailed by legal regulation. This is one of the functions of traditional administrative law and extends to data protection law[51]. A similar rationale explains the European option to regulate processing done in the private sector.

Data protection regulations mainly[52] belong to the tools of transparency, as opposed to the protection of privacy that pertains to the tools of opacity. The sheer wordings of the data protection principles (the

51 P. BLUME, "The Citizens" Data Protection", *l.c.*, pp. 2-3.

52 There are exceptions: namely those parts of the data protection regime that provide for a prohibition of processing (*e.g.* sensitive data, secretly collected personal data) actually fall under a privacy or opacity ruling. See *infra*.

fairness principle, the openness principle and the accountability principle, the individual participation principle, [...]) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice. The data protection regulations create a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal[53]. As such these regulations implicitly accept that a processing of personal data is closely linked to the exercise of power and that it facilitates its establishment.

That explains why European data protection regulations were immediately conceived as applicable both in the public and in the private sector. The power of those, be it in the public or in the private sector, who process personal data concerning others (whether with the help of information technology or not) is generally already greater to begin with. The stream of personal data primarily flows from the weak actors to the strong. Citizens not only need to provide information to the authorities, but they also need to do so as tenant, job seeker, customer, loan applicant and patient. That is precisely why legal tools of transparency and accountability under the form of data protection regulations were devised for application both in the public and in the private sector.

### 4.3 Data protection as an opacity tool?

At first sight privacy and data protection are identical tools in nature, since the Data Protection Directive foresees a system of general prohibition, requiring some conditions to be met for "making data processing legitimate". The impression is given that the basic logic behind is of a prohibitive nature: "no processing, unless...". This understanding is however not correct for, firstly, the directive was heavily inspired by and had to accommodate existing national data protection regulations which were not based upon the prohibition principle. Secondly, the Data Protection Directive provides for a catch all ground for private data processing in its art 7 f. According to this article personal data can be processed without consent of the data subject if the processing "is necessary for the purposes of the legitimate interests pursued by private interests, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject".

53 An outright processing ban effectively applies only to special categories of sensitive personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

For some authors this article even covers the processing of data for direct marketing purposes. Indeed such an article obliges a serious analyst to doubt and even refute the idea that the processing of personal data is in principle prohibited or dependent of the consent of the data subject. Art. 7 f in fact spans the whole scale of possibilities and can obviously "make data processing legitimate" for every thinkable business interest.

Nevertheless, exceptions from this general rule do exist. For instance, a prohibitive rule applies to "sensitive data" (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual preference). The core of the underlying motive is that the processing of such sensitive data bears a supplementary risk of discrimination. The prohibition is nonetheless never absolute but derogations are (in principle) only possible in strictly defined circumstances, for example for reasons of national security. Another example can be found in Art. 15 Data Protection Directive[54], inasmuch as this article can be construed as the prohibition of decision making affecting persons solely on the basis of profiles. But again, both prohibitive features are accompanied by numerous exceptions that do not set strong limits to the targeted actions.

A third opacity tool in data protection can be found by an interpretation of the purpose specification principle. This principle, at the heart of data protection as it existed in many countries before the European Data Protection Directive came into force, states that the purposes for which personal data are collected should be legitimate and should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfilment of those purposes. Preventive control of the intention of

54 According to this article every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data". The article refers to automated processing of data "intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.". The goal is to guarantee everyone's participation in important personal decisions. A dismissal based purely on the data from the company time clock is, as a result, unacceptable. It applies also to the rejection of a jobseeker based on the results of a computerised psycho-technical assessment test or to a computerised job application package. Those decisions have to take professional experience or the result of a job interview into account. The automated test is insufficient and it applies to such sectors as banking and insurance. The EU member states have to enact provisions that allow for the legal challenge of computerised decisions and which guarantee an individual's input in the decision-making procedures. However member states are allowed to grant exemptions on the ban on computerised individual decisions if such a decision "(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests".

the controller and prohibition of illegitimate use was at the heart of data protection. The idea was not wholly new, since Article 8 ECHR holds that infringements of privacy can only be organised by law for legitimate purposes. In the past, when data was used mostly for only a single purpose, the logic behind the principle could be upheld without too much difficulty. Today, in the new economy and in a public sector ready for e-government, data is used for multiple purposes and much more intensely and effectively than ever before. Clearly these evolutions have influenced the drafting of the Data Protection Directive.

The fundamental purpose limitation principle is now stated in Article 6 (1b) of the Data Protection Directive. Compared to the situation in, *e.g.*, Belgium before the Data Protection Directive, the wordings are weakened. It is now said that subsequent use of data should be limited to the fulfilment of the initial purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. This loosening of the purpose specification principle, coupled to the numerous possibilities in the Directive to render processing legitimate by obtaining consent, can be interpreted as a shift from prohibitive to channelling logic. Transparency seems to have replaced legitimacy as the core value of data protection. Whatever processing has been rendered transparent is legitimate.

### 4.4 The charter of fundamental rights of the European Union

The European Convention for the Protection of Human Rights (ECHR) plays a crucial role regarding the protection of privacy. However, in the ECHR there is no article that explicitly protects personal data. Although the organs of the ECHR have recalled on several occasions that data protection is an issue which falls within the scope of Article 8 ECHR[55], they have also held that not all aspects of the processing of personal data are protected by the Convention and that not all personal data are worthy of privacy protection[56]. In recent cases such as *Amann, Rotaru* and *P.G. and J.H. v. the United Kingdom*, the European Court seems to remedy to this by applying a

55 For instance: European Commission on Human Rights, *Lundvall v. Sweden*, 11 December 1985, case 10473/83, *D.R.*, v. 45, p. 130.

56 For a detailed discussion: P. DE HERT, "Mensenrechten en bescherming van persoonsgegevens. Overzicht en synthese van de Europese rechtspraak 1955-1997" [Human Rights and Data Protection. European Case-Law 1995-1997], in *Jaarboek* ICM 1997, Antwerpen, Maklu, 1998, pp. 40-96.

very broad definition of privacy[57]. However, these cases should be carefully interpreted. A closer reading shows that the old distinction between "data that merit protection" and "data that does not" is still operating. Also, the reference to existing data protection treaties is formulated in a way that leaves room for discretion.

Very recently the proper role of data protection has received constitutional recognition in Article 8 of the 2000 Charter of Fundamental Rights of the European Union[58]. Unlike in the ECHR the Charter did provide for a separate right to data protection next to the right to a private life for the individual. The Charter contains an uninspired copy of Article 8 ECHR, namely Article 7 which states that: "Everyone has the right to respect for his or her private and family life, home and communications". But the next and separate Article 8 of the Charter focuses explicitly on the protection of personal data. It inspiringly states:

> Everyone has the right to the protection of personal data concerning him or her. 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 that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

This recognition of a constitutional right to data protection in the EU Charter should be welcomed for several reasons. To begin with it allows for a sensible constitutional division of labour. Data protection explicitly protects values that are not at the core of privacy, such as the requirement

57 For instance in *Amann v. Switzerland*, judgement of 16 February 2000, § 65-57: "The Court reiterates that the storing of data relating to the 'private life' of an individual falls within the application of Article 8 § 1 (see the *Leander v. Sweden* judgement of 26 March 1987, Series A n. 116, 22, § 48). It points out in this connection that the term 'private life' must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature (see the *Niemietz*, § 29 and *Halford v. United Kingdom,* judgement of 25 June 1997, § 42). That broad interpretation tallies with that of the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985, whose purpose is 'to secure in the territory of each Party for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him' (Article 1), such personal data being defined as 'any information relating to an identified or identifiable individual' (Article 2). In the present case the Court notes that a card was filled in on the applicant on which it was stated that he was a 'contact with the Russian embassy' and did 'business of various kinds with the company [A.]' (see paragraphs 15 and 18 above). The Court finds that those details undeniably amounted to data relating to the applicant's 'private life' and that, accordingly, Article 8 is applicable to this complaint also".

58 Http://europa.eu.int/comm/justice_home/unit/charte/en/charter02.html.

of fair processing, consent or legitimacy. The explicit recognition in the new provision of a "right of access to data that has been collected concerning him or her, and the right to have it rectified" solves legal problems unanswered by the case law of the European Court of Human Rights. Equally, there is no ground in this case law for a right to have compliance with (all) data protection rules controlled by an independent authority, as is foreseen by the last paragraph of the new provision[59]. Furthermore, the Charter extents the protection of personal data to private relations and the private sector[60].

The recognition of a separate right to data protection, next to privacy, is also more respectful of the different European constitutional traditions. Contrary to countries such as Belgium that have linked data protection from the start to privacy, countries such as France and Germany, lacking an explicit right to privacy in their constitution, have searched and found other legal anchors for the recognition of data protection rights. French data protection is therefore based on the right to liberty, whereas German data protection is based on the right to have human dignity recognised. Equally, the roots of American data protection are to be found in public law, viz. fair information practices. Hence, there are several grounds for data protection, which does not allow the use of one general privacy label.

Last and foremost, data protection has grown in response to problems generated by new technology. It brings no added value to reduce all these responses to "privacy". Other values and concerns are also at play. Take for instance the right not to be discriminated against that is protected by Article 15 of the European Data Protection Directive[61]. There is also a special regime for "sensitive data" in the Directive prohibiting processing of data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs and so on. The connection with rights and liberties such as the freedom of religion, freedom of conscience and the political freedoms is obvious.

59 Article 13 ECHR (right to an effective legal remedy) does not create an independent right. The European Court refuses to consider issues under this provision, when there is no violation of another right of the ECHR. See *infra*.

60 Cf. Y. POULLET, "Pour une justification des articles 25 et 26 en matière de flux tranfrontières et de protection des données" in *Ceci n'est pas un juriste [...] mais un ami. Liber Amicorum Bart De Schutter*, M. COOLS, C. ELIAERTS, S. GUTWIRTH, T. JORIS & B. SPRUYT (editors), Brussels, VUBPress, 2003, p. 278.

61 According to this article every person has the right "not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data". The article refers to automated processing of data "intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.". The goal is to guarantee everyone's participation in important personal decisions. A dismissal based purely on the data from the company time clock is, as a result, unacceptable.

## 5 THE SHIFT FROM OPACITY TOWARDS TRANSPARENCY IN EUROPEAN HUMAN RIGHTS LAW

### 5.1 European human rights law and the legality requirement

After having discussed the respective functions of privacy and data protection in the European democratic state, let us now turn to the European legal landscape of human rights law. In our introduction we mentioned the crucial role of the European Convention for the Protection of Human Rights regarding the protection of privacy. This Convention is designed to protect individuals' fundamental rights and freedoms and provides for a judicial procedure which allows individuals to bring actions against governments, if they consider that they are the victims of a violation of the Convention. After the exhaustion of national remedies, individual complainants have direct access to an international court, the European Court of Human Rights in Strasbourg.

Article 8 ECHR, the privacy article of the Convention, states:

> (1.) Everyone has the right to respect for his private and family life, his home and his correspondence. (2.) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

This provision, partly copied in Article 7 of the European Union Charter of Fundamental Rights[62], is the source for EU legislation dealing with privacy and the protection of personal data, as well as of national legislation. Article 8 of the ECHR does not formulate privacy as an absolute right. Exceptions are made possible in the second paragraph of the provision, but the drafters of the Convention took care to provide safeguards against possible abuse of the right to formulate exceptions. Therefore, if any exception to the protection of data privacy is adopted respect has to be given to the conditions laid down in Article 8.2 of the Convention, that is, any invasion of privacy for a legitimate reason (for purposes of criminal investigation, usually the prevention of

62 This Article of the EU-Charter states that: "Everyone has the right to respect for his or her private and family life, home and communications".

crime) must be adopted "in accordance with the law" and when "necessary in a democratic society". Those requisites are cumulative[63].

Article 8 of the ECHR has been largely commented by legal authorities and applied by the European Court of Human Rights in Strasbourg[64]. We have analysed this case-law elsewhere[65], and limit ourselves to observations pertinent to the theme of this paper.

The large or extensive interpretation of the provision by the European Court is not limited to the scope of the notion of "privacy" included in Article 8.1 of the Convention[66]. The first requisite of Article 8.2 of the Convention, viz. a restriction must be adopted "in accordance with the law", has been interpreted in a non-formal way. In *Kruslin* the Court held, in the context of

63 "The interference was not therefore 'in accordance with the law' as required by the second paragraph of Article 8 and there has been a violation of this provision. In these circumstances an examination of the necessity of the interference is no longer required", *P. G. and J. H. v. The United Kingdom*, judgement of 25 September 2001, § 63. "The Court concludes that the interference cannot therefore be considered to have been 'in accordance with the law' since Swiss law does not indicate with sufficient clarity the scope and conditions of exercise of the authorities' discretionary power in the area under consideration. [...] Having regard to the foregoing conclusion, the Court does not consider it necessary to examine whether the other requirements of paragraph 2 of Article 8 were complied with"; *Amann,* § 19. See also: V. Coussirat-Coustere, "Article 8 § 2", in L. Pettiti, E. Decaux & P. Imbert (editors), *La Convention Européenne des Droits de l'Homme. Commentaire article par article*, Economica, 2e Edition, Paris, 1999, pp. 323-351.

64 The rights and freedoms of the Convention are formulated in a broad fashion. In order to apply them to concrete situations the Strasbourg authorities employ a number of interpretation techniques. Thus, the Court may embark on a grammatical analysis of the provision at issue, or apply a systematic interpretation; it may refer to the *travaux préparatoires* of the Convention or rather interpret the Convention according to "present-day conditions". An important element in this respect is also whether consistent State practice exists in regard to the issue at hand. One of the most remarkable aspects of the Strasbourg case-law is its dynamic character. On numerous occasions the Court emphasised that the Convention is "a living instrument which should be interpreted according to present-day conditions". See, *e.g.*, *Tyrer v. the United Kingdom*, judgement of 25 April 1978, § 31; *Marckx v. Belgium*, judgement of 13 June 1979, § 41; *Dudgeon v. the United Kingdom,* judgement of 22 October 1981, § 60; *Soering v. the United Kingdom*, judgement of 7 July 1989, § 102; *B. v. France*, judgement of 25 March 1992, §§ 45-48 and *Salesi v. Italy,* judgement of 26 February 1993, § 19. This culminated in 1995 when the Court held that the Convention "cannot be interpreted solely in accordance with the intentions of their authors as expressed more than forty years ago [...] at a time when a minority of the present Contracting Parties adopted the Convention" (*Loizidou v. Turkey (prel. obj.)*, judgement of 23 March 1995, § 71). In a similar vein the Court has repeatedly stressed that the Convention is intended to guarantee "not rights that are theoretical or illusory but practical and effective"; see, *e.g. Airey v. Ireland*, judgement of 9 September 1979, § 24 and *Soering*, § 87. It will be clear that this approach opens the way for expanding the protection offered by the Convention.

65 For a detailed analysis of the case-law, see P. DE HERT, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie* [Article 8 ECHR and the Law in Belgium. Protection of Privacy, House, Family and Correspondence], Gent, Mys en Breesch Uitgeverij, 1998, 367 p. and P. DE HERT, "Artikel 8 EVRM. Recht op privacy" [Article 8 of the Convention on Human Rights. The Right to Privacy] in J. VANDE LANOTTE & Y. HAECK (editors), *Handboek EVRM. Deel 2 Artikelsgewijze Commentaar*, Antwerp-Oxford, Intersentia, 2004, pp. 705-788.

66 *Rotaru v. Romania*, judgement of 4 May 2000; *P.G. and J. H.*, etc.

French criminal procedure, that the notion of "law" comprises written as well as unwritten law[67].

This questionable move towards flexibility (*infra*) has been partly compensated by the theory of the Court that the notion of "law" implies qualitative requirements, notably those of "accessibility" and "foreseeability". Interference by the executive with the rights and freedoms of the individual should not be permitted unless there is a clear legal basis to do so. It is not sufficient for Member States just to adopt a written law. According to the Court a legal and fully transparent legal basis must exist for justifying a measure limiting privacy rights. The object of the legal basis must also be specific. Any extensive exploratory or general surveillance (for example, of persons or of data) is prohibited[68]. A formal legal basis is not sufficient. The law, – be it case law or statute – must be of a certain quality: foreseeable (sufficiently detailed) and accessible and providing remedies for the citizen[69]. Partly these three quality requirements follow from the more general principle of the "rule of law". This principle requires effective safeguards against arbitrary interference by the authorities.

### 5.2 The success of the legality requirement

Many cases under Article 8 involve the legality requirement. Often the Court found that the safeguards needed to comply with the requirement were lacking[70]. While in continental "civil" legal systems and culture it is regarded as self evident that interference with the individual citizen by the state requires an explicit basis in law, common law systems take the opposite view: everything is allowed unless forbidden. Therefore, the full implementation of the ECHR required of the United Kingdom a substantial

67 See *Kruslin v. France*, judgement of 24 April 1990, §§ 27-36. At the same time the Court has realistically accepted that the wording of statutes is not always precise and that excessive rigidity must be avoided (*Kokkinakis v. Greece*, judgement of 25 May 1993, § 40; *S.W. v. UK*, judgement of 22 November 1995, § 36).

68 This principle has been constantly repeated by the European Court of Human Rights in what concerns electronic surveillance and wire tapping; see notably recently *Klass and others v. Germany*, judgement of 6 September 1978 and *Khan v. U.K.,* judgement of 12 May 2000.

69 The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law. It also requires that the measure under examination comply with the requirements laid down by the domestic law providing for the interference. See *e.g. Kopp v. Switzerland*, judgement of 25 March 1998, § 55; *Perry v. United Kingdom,* judgement of 17 July 2003, § 55.

70 See, *e.g.*, *Kruslin*, §§ 30-35 and *Niemietz*, § 37.

cultural *volte face*[71], at least as far as the rules governing police powers are concerned[72]. A similar cultural or psychological revolution has taken place in the Civil law systems, such as France and Belgium, where historically a central role in law enforcement was accorded to the investigating judge, a person believed to be above all suspicion due to his independent position. The 1990 *Kruslin* and *Huvig* cases scattered the holy image of the investigating judge, unknown to Common Law systems. A provision in the French Code of Criminal Procedure giving this judge "all the necessary powers to seek the truth" was declared incompatible with Article 8 of the Convention. Even the powers of the investigative judge have to be made foreseeable and accessible[73].

The case-law regarding the legality requirement has also enabled the European Court to make clear that assessing privacy infringements is not only a question of transparency, but also of accountability. The requirement of foreseeability in particular has allowed the Court to fuse the due process requirements of Article 6 ECHR and the effective remedy requirement of Article 13[74] into the privacy requirements of Article 8 ECHR. With regard to telephone tapping and other investigation techniques this has brought the Court to a very detailed set of conditions that have to be fulfilled by the legislatures and have to be respected by law enforcement authorities. These conditions oblige legislators to explicitly and precisely foresee which categories of persons can be the object of the measures, for which incriminations the measures can be taken, how long they can last, how reports/log books about the measures must be made up and, in case of later suspension of prosecution or acquittal, be destroyed. However, this has at least one important drawback: any measure of telephone tapping will be deemed to be legitimate if it meets the conditions. It can thus also be feared that such a channelling "transparency" approach encroaches upon the normative "opacity" that privacy is meant to protect.

---

71 The course of the events from *Malone* to the Regulation of Investigatory Powers Act 2000 is a *locus classicus*. A violation was found of Article 8 ECHR in a case concerning interception and metering of telecommunication, on the grounds that a legal basis as required by Article 8 was absent in English law. The Interception of Communications Act 1985 was an attempt to remedy for this. Cf. *Malone v. United Kingdom*, judgement of 2 August 1984.

72 P. ALLDRIGDE & CH. BRANTS, "Introduction" in P. ALLDRIGDE & CH. BRANTS (editors), *Personal Autonomy, the Private Sphere and the Criminal Law. A Comparative Study*, Oxford, Hart Publishing, 2001, p. 13.

73 P. DE HERT, "Het recht op een onderzoeksrechter in Belgisch en Europees perspectief", *l.c.*, pp. 155-198.

74 This article reads as follows: "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority [...]".

### 5.3 A critical comment about the Strasbourg focus on the legality requirement

Undoubtedly the legality requirement has important merits and by imposing it for police powers (inter alia) that touch upon certain human rights its basic goal is realised. Although we suggested in our introduction that privacy is not a central value of criminal law enforcement, the aforementioned case-law shows that privacy has an impact on criminal law and has the ability to enrich it[75]. Also, the way the European Court handles this requirement is not without intelligence and constitutional wit. But strictly speaking the legality requirement in Article 8 ECHR has nothing to do with privacy[76]. Privacy is not about legality, it is about power and how to stop it. This brings us to the ambiguity we mentioned in our introduction when referring to the vast body of privacy case-law developed by the European Court of Human Rights in Strasbourg and also to a critical attitude regarding the dominant privacy focus on the legality requirement laid down in Article 8 of the Convention[77].

As an opacity tool Article 8 of the ECHR is not an ideal starting position, especially when compared to *e.g.* the U.S. First Amendment that foresees no explicit exceptions. To start with, the right to respect for privacy as enshrined in the Convention is not absolute. The flexible notion of respect is informed by the interests of national security, public safety, the economic well being of the country, prevention of disorder and crime, protection of public morals and the rights and freedom of others. This broadly formulated list of legitimate grounds to restrict privacy in Article 8.2 of the Convention potentially allows for a broad governmental discretion. The nature of the privacy right enshrined in the Convention is therefore not clear from the start. Its use and interpretation decide whether and when this provision functions as a power blocking tool. The responsibility of the European Court, as a last interpreter of the Convention, is considerable in this respect.

---

75 Generally speaking there is no legality requirement within the law of criminal procedure. Although we observed that in continental "civil" legal systems and culture it is regarded as self evident that interference with the individual citizen by the state requires an explicit basis in law, almost no countries exist, with the exception of Germany and the Netherlands, where the Codes of Criminal Procedure state that all actions of the law enforcement authorities need an explicit basis in law. Also in human rights law, especially with regard to the law of criminal procedure, there is no "human" right to have all police powers based upon a law. A general requirement for legality with regard to all law enforcement powers is, for instance absent in the ECHR. By saying that certain powers touch upon privacy a bit of this "principle" can however be read into the Convention.

76 The requirement can also be found in the three subsequent articles of the Convention.

77 We borrow from P. DE HERT, "Strafrecht en privacy. Op zoek naar een tweede adem" [Criminal Law and Privacy. Searching for a New Breath], *Rechtshulp. Maandblad voor de sociale praktijk*, 2003/10, pp. 41-54.

We argued above that data protection regulations should be regarded as transparency tools, whereas the protection of privacy pertains to the tools of opacity. It is useful and necessary not to blur this distinction since each tool has it proper logic. However, the focus on the requirement "in accordance with the law" has turned Article 8 ECHR into a transparency-promoting vehicle. One can regret, but understand, the habit of the Court not to go any further with its investigations once it has decided a case merely on the basis of the requirement "in accordance with the law"[78]. However, one cannot understand its insistence on the quality of the law in the context of Article 8 of the Convention and its disregard of the formal status of the legal basis that is used by the Member States to justify certain privacy limitations. We recall that even within the Civil Law systems it is not always required to have a formally voted law. Case-law and other legal texts may do, as long as they fulfil the quality requirements. Democratically there is a loss. Insisting on the content of law, rather than on the formal basis of law, has allowed the Court to declare certain regulations "in accordance with the law" that have not even been debated and approved by a parliament[79].

### 5.4 The danger of proceduralisation

Constitutionally there is also loss, because the proper division of labour between the existing human rights has not been respected[80]. We have already said that the requirement of foreseeability has allowed the Court to fuse the due process requirements of Article 6 ECHR and the effective remedy requirement of Article 13 into Article 8 ECHR. This approach has been detrimental for both provisions, especially Article 13. Elements of

78 The other requirements of Article 8.2 of the Convention, especially the requirement that privacy limitations need to "necessary in a democratic society", are often not checked by the Court, when a breach of the legality requirement is found. The Convention organs treat the requirements as successive hurdles. This means that where they find that a measure complained of is not "in accordance with the law", then they do not proceed to examine whether the measure satisfies the requirement of "necessity in a democratic society". For instance in *P.G. and J.H.*, § 38: "As there was no domestic law regulating the use of covert listening devices at the relevant time [...], the interference in this case was not 'in accordance with the law' as required by Article 8 § 2 of the Convention, and there has therefore been a violation of Article 8 in this regard. In the light of this conclusion, the Court is not required to determine whether the interference was, at the same time, 'necessary in a democratic society' for one of the aims enumerated in paragraph 2 of Article 8." See also: I. CAMERON, *National Security And The European Convention On Human Rights*, The Hague/London/Boston, Kluwer Law International, 2000, p. 36.

79 See: P. BLONTROCK & P. DE HERT, "Telefoontap: Tournet, Peureux, Hüvig, Kruslin et les autres", *Rechtskundig Weekblad*, 1991-1992, 865-871 and I. Cameron, *o.c.*, p. 34.

80 The ECHR recognises some procedural rights, such as the right to a fair trial (art 6) and the right to an effective remedy (art. 13) next to substantial rights like privacy, freedom of expression, conscience, religion and assembly (art. 8 to 11).

procedural rights are borrowed to construe a substantive norm, and the result is used to interpret the procedural rights narrowly[81].

Of course, this situation is far from evident. The two categories of rights in the Convention, procedural rights and substantive rights, were originally conceived as being complementary, but today it can be held that, in the case law of the Court, the two categories have merged or "conpenetrated"[82]. More and more the respect of a number of procedural conditions concerning transparency, impartiality, accessibility, [...] has become an essential condition for a legitimate restriction of a substantial conventional right. According to Tulkens and Van Droogenbroeck this "proceduralisation of substantial rights" has both positive and negative effects. It is positive inasmuch as this evolution contributes to the objectivity and credibility of the Court's control as it compels the Court to take "distance" from the facts of the case: prior to an inquiry into the merits and facts of the case (entailing a discussion of the state's *margin of appreciation*), the Court will merely check if the contested decision or measure meets all formal requirements. Indeed, such a demarche also meets the principle of the subsidiarity of the international review. On the other hand, negatively speaking now, Tulkens and Van Drooghenbroeck fear that a procedural review might come to be substituted for the substantial review by a procedural one: the proceduralisation of substantial rights might well lead to a situation wherein the Court would definitively stop to check and review restrictions of fundamental rights in the light of the values and norms enshrined in the ECHR[83].

If proceduralisation bears the advantage of objectivity and impartiality, it also leads just as surely to the formalisation, bureaucratisation and depoliticisation of human rights questions: meeting formal constraints and conditions is never a hurdle too high to take. This is convincingly illustrated

81 In *Klass* the Court introduced a heavily criticised restrictive or "relative" approach. The Court considered that Article 13 has a subsidiary character in relation to Article 8. Thus Article 13 could not be interpreted so as to nullify the efficacy of the measures of secret surveillance already found to be compatible with Article 8. The Court stated that "an effective remedy [...] must mean a remedy which is as effective as can be having regard to the restrictive scope for recourse inherent in any system of secret surveillance"; *Klass*, § 69. See the consequences of this approach for judicial checking on secret surveillance: I. Cameron, *o.c.*, pp. 36-39.

82 In this context Françoise Tulkens and Sébastien Van Droogenbroeck use the term of "*conpénétration*". They come to the conclusion that "chacune des dispositions conventionnelles consacrant un droit substantiel est susceptible de sécréter des garanties d'ordre procédural contribuant à l'effectivité du droit concerné et attachées davantage aux processus décisionnels qu'aux décisions proprement dites"; FR. TULKENS & S. VAN DROOGENBROECK, "La cour européenne des droits de l'homme depuis 1980. Bilan et orientations" in *En toch beweegt het recht*, W. DEBEUCKELAERE & D. VOORHOOF (editors), *Tegenspraak-cahier 23*, Brugge, Die Keure, 2003, p. 224.

83 FR. TULKENS & S. VAN DROOGENBROECK S., *l.c.*, pp. 223-227.

by the telephone tapping case-law (*Klass, Malone, Huvig, Kruslin*, [...]) which has led to the devising of a detailed and elaborate set of conditions that taps must fulfil in order to be considered as legitimate. But the other side of the coin is that the question of the necessity of such practices in a democratic society fades away into the background: it is enough that the tapping meets all the formal conditions [...] Proceduralisation might well bring the erosion of recognised rights[84].

If there are good reasons for this process of proceduralisation, the Court has not provided them[85]. The unfortunate treatment of Articles 6 and 13 in *Klass* seem to be inspired by the will to accept secrecy and to strain the paradigmatically adversarial nature of the judicial guarantees set forth in Article 6[86]. The attempt to read Article 6 notions in the legality requirement

84 Of course, we are well aware that emphasising the substance of the fundamental rights also has dangerous drawbacks. Indeed, such an approach implies that Court determines and describes what these rights consist in, which is only possible through the identification of the values upon which the ECHR relies. But which are these values? What is the meaning of words like "democracy" and "rule of law" setting the broader environment in which the "fundamental rights and freedoms" must be concretised? Which political philosophy lies at the roots of the Convention: is it the aim to implement a minimal and liberal state wherein individual liberty is the most important value? Or does the Convention aim at the realisation of a more republican or even communitarian state driven by the public interest or common values? Or is it something between the two: a kind of relational or polyphonic state?

85 It is possible to find some rationale to transform Article 8 into a procedural norm. In *Silver and Others v. United Kingdom* the Court made it clear that a law which "allows the exercise of unrestrained discretion in individual cases will not possess the essential characteristics of foreseeability and thus will not be a law for present purposes. The scope of the discretion must be indicated with reasonable certainty"; *Silver and Others v. United Kingdom*, judgement of 25 March 1983, § 88-89. In cases such as *Klass, Huvig* and *Kruslin* the Court has also stated that adequate safeguards also must exist against abuse of the discretion established by law (*Klass*, § 63*, Huvig v. France*, judgement of 24 April 1990, § 34 and *Kruslin,* § 35).

86 In *Klass* it accepted that a secret telephone tapping measure was compatible with article 8 ECHR. One step further it decided that a legitimate *and* secret telephone tap cannot violate articles 6 and 13 ECHR. In their submission the applicants argued that the legislation violated Article 6 insofar as it did not require notification to the person concerned in all cases after the termination of surveillance measures and excluded recourse to the courts to test the lawfulness of such measures. The Court simply refused to consider the complaint: once decided that a system of secret surveillance without notification does not contravene Article 8, the right to judicial control in Article 6 does not apply (cf. *Klass*, § 75). But these articles do not provide for the same restrictions and exceptions as article 8, which permits us to conclude with François Rigaux that'(e) n développant son raisonnement à partir de l'équilibre entre la règle et l'exception dans l'article 8 la Cour introduit la même exception dans les articles 6 et 13 qui ne la connaissent pas". Cf. F. RIGAUX, *La protection de la vie privée et des autres biens de la personnalité*, Brussel/Parijs, Bruylant/L. G. D. J., 1990, 201. See also: E. A. ALKEMA, "Klass e.a. tegen de Duitse Bondsrepubliek", *Ars Aequi*, 1979, 323 and P. DE HERT, *Art. 8 E.V.R.M. en het Belgisch recht, o.c.*, 342-343. This is even more disturbing because the effect of articles 6 and 13 upon secret investigative methods should not be underestimated. Both articles foresee the right to have conflicts and disputes reviewed by an independent and impartial tribunal. This would imply that persons who were subjected to secret measures (and hence did not know about it) should afterwards be informed of these measures even if they remained without results. See also A. H. J. SWART, "Anoniem gerechtelijk vooronderzoek", *Ars Aequi*, 1984, 335. If this guarantee is lacking, only these subjects of the said secret measure who will be prosecuted later will be informed about the way data about them has been collected. Comp. "Au contraire, si les éléments recueillis sont insuffissants pour que des poursuites puissent être intentées ou que l'autorité compétente estime cellesci inopportunes, les organes du pouvoir exécutif ont le pouvoir discrétionnaire de conserver le secret sur les mesures prises à l'égard de faits qui, par hypothèse, n'ont entraîné aucune poursuite alors que, seul, leur caractère punissable justifiait que la mesure fût prise";

of Article 8 seems to be the result of a more or less explicit refusal by the Court to test the reasonableness of a system of secret surveillance provided for by law and in particular to test the requirement of subsidiarity. The citizen gets procedural guarantees as a compensation for the lack of testing of the reasonableness of the intrusion[87]. We recall that this case law misreads the convention by fusing together two (or three) provisions, which are motivated by very different ideas and do not run into each other. Article 8, unlike Article 6, has a general scope, while Article 6 is limited to conflicts about 'the determination of civil rights and obligations or of any criminal charge against" a person. Article 8 is about substantive issues, Article 6 about procedural rights. Unlike the fair trial clause, the privacy right speaks not only to procedural fairness but (mainly) to substantive fairness. It is therefore far more sensible to try to read the privacy right, with its open-ended nature, in light of other *substantive* norms contained in the Convention.

Ian Cameron is obviously of the same opinion. This author holds that these procedural requirements should not be seen as a feature of the legality requirement, but rather as a requirement of Article 13 and/or a requirement

F. RIGAUX, *o.c.*, 200. This looks a little bit like a carte blanche for secret measures. In sum, in *Klass*, the interpretation of the substantial right to privacy leads to a weakening of the procedural guarantees of the fair trial. For Rigaux *Klass* is a "jugement d'opportunité politique". In the Malone case also, the Court avoided reviewing a telephone tapping measure from the perspective of art. 13 arguing that this was unnecessary because it had already decided a violation of art. 8 ECHR. Recently, in *Perry* the Court sharply separated the privacy right from the fair trial right. *Perry*, § 48. "Though the Government has argued that it was the quality of the law that was important and that the trial judge ruled that it was not unfair for the videotape to be used in the trial, the Court would note that the safeguards relied on by the Government as demonstrating the requisite statutory protection were, in the circumstances, flouted by the police. Issues relating to the fairness of the use of the evidence in the trial must also be distinguished from the question of lawfulness of the interference with private life and are relevant rather to Article 6 than to Article 8. It recalls in this context its decision on admissibility of 26 September 2002 in which it rejected the applicant's complaints under Article 6, observing that the obtaining of the film in this case was a matter which called into play the Contracting State's responsibility under Article 8 to secure the right to respect for private life in due form".

87 See *Klass*, § 49 & 50: "49. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. *It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field* (cf., mutatis mutandis, the *De Wilde, Ooms and Versyp* judgement of 18 June 1971, § 93, and the *Golder* judgement of 21 February 1975, § 45; cf., for Article 10 § 2, the *Engel and others* judgement of 8 June 1976, § 100, and the *Handyside* judgement of 7 December 1976, § 48). Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. 50. *The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.* This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law" (italics are added). Comp. these paragraphs with §76 of the *Peck* judgement; *Peck v. United Kingdom,* judgement of 28 January 2003.

of "necessity in a democratic society"[88]. We prefer the first option. Article 8 of the Convention is no place for procedural questions. The framers of the Convention have designed other articles for that purpose. The transformation of Article 8 into a source of procedural rights and procedural conditions takes it away from the job it was designed for, viz. to prohibit unreasonable exercises of power and to create zones of opacity.

### 5.5 A requirement fundamental to opacity: necessary in a democratic state

We observed that a lot of important Article 8 cases are "solved" by concentrating on issues concerning transparency. The question whether a certain practice is "necessary in a democratic society" is often not answered by the Court, when a breach of the legality requirement is found (*supra*). However, checking on the legality requirement is of a fundamentally different nature than checking on the requirement "necessary in a democratic society". Only the latter requirement deals with the political question whether power should be limited, stopped or prohibited or, in other words, whether "opacity" must be protected. Even if a restriction of privacy is foreseen by law and serves an objective summed up in article 8 § 2 ECHR, this restriction must still be "necessary in a democratic society" and shouldn't reach further than what is strictly necessary[89]. This condition inevitably implies an ultimate balancing of interests, a value judgement and/or a substantial choice, which cannot be found in an exegetic reading of the text, nor in a strict application of logical rules[90].

Such a balancing of interests, which takes the weight of fundamental rights and freedoms duly into account, is essential[91]. It allows for the exercise of the political function of human rights. The need to limit power through opacity tools explains the importance of the requirement "necessary in a democratic society". Behind this requirement lies the true constitutional question with regard to law enforcement and privacy: is there a justifiable necessity for the law enforcers to break into the privacy and to lift the

88 I. Cameron, *o.c.*, 34.

89 About this condition see K. RIMANQUE, "Noodzakelijkheid in een democratische samenleving – een begrenzing van beperkingen aan grondrechten", in *Liber Amicorum Frédéric Dumon,* Antwerp, Kluwer Rechtswetenschappen, 1983, deel II, p. 1220.

90 K. RIMANQUE, *l.c.*, p. 1229.

91 Cf. S. GUTWIRTH, "De toepassing van het finaliteitbeginsel van de Privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens" [The application of the purpose specification principle in the Belgian data protection act of 8 December 1992], *Tijdschrift voor Privaatrecht*, 4/1993, pp. 1409-1477.

opacity of the individual? In the context of Article 10 ECHR (freedom of expression) the Court has observed that "necessary [...] is not synonymous with *indispensable,* neither has it the flexibility of such expressions as *admissible, ordinary, useful, reasonable* or *desirable,* but that it implies a *pressing social need"*[92].

Obviously this interpretation is too far reaching for the European judges as regards privacy. Not many cases under Article 8 repeat this kind of exercises. Almost always the requirement of "necessity" is brought back to the question of proportionality, in some cases supplemented by the requirement that the reasons for the interference are relevant and sufficient[93]. Only in the recent *Peck* judgement can one find some word games referring to the semantic exercise in the context of Article 10 discussed above[94]. What is "proportionate" will depend on the circumstances. According to M. Delmas-Marty, in determining proportionality the Court takes particularly into account the nature of the measure taken (its reach, whether it is general of absolute, its adverse consequences, the scope for abuse of the measure), whether the state concerned could have taken other measures or implemented them in a less drastic way, the status of the persons involved whose rights can legitimately be subject to greater limitation (*e.g.* prisoners) and finally, whether there are any safeguards which can compensate for the infringement of rights which a measure can create[95].

However, the Strasbourg judges are too hesitant and reluctant to really address these issues. They clearly prefer the much more secure test of

92 *Handyside v. United Kingdom*, judgement of 7 December 1976, § 48.

93 P. DE HERT, *Artikel 8 EVRM en het Belgisch recht*, *o.c.*, 40-60. Compare with §76 of the *Peck* judgement: "In determining whether the disclosure was "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify the disclosure were "relevant and sufficient" and whether the measures were proportionate to the legitimate aims pursued"; *Peck v. United Kingdom,* judgement of 28 January 2003.

94 See the use of the term "pressing social need" in the following quote: "In such circumstances, the Court considered it clear that, even assuming that the essential complaints of *Smith and Grady* before this Court were before and considered by the domestic courts, the threshold at which those domestic courts could find the impugned policy to be irrational had been placed so high that it effectively excluded any consideration by the domestic courts of the question of whether the interference with the applicants" rights answered a pressing social need or was proportionate to the national security and public order aims pursued, principles which lay at the heart of the Court's analysis of complaints under Article 8 of the Convention; *Peck*, § 100.

95 M. DELMAS-MARTY, *The European Convention for the Protection of Human Rights,* Dordrecht, 1992, 71 quoted by I. Cameron, *o.c.*, 26. About proportionality see also: S. Gutwirth, "De toepassing van het finaliteitbeginsel [...] [The application of the purpose specification principle ...]", *l.c.*, § 20; S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droit de l'homme. Prendre l'idée simple au sérieux*, Bruxelles, Bruylant/Publications des FUSL, 2002, 790 p. and W. Van Gerven, "Principe de proportionnalité, abus de droit et droits fondamentaux", *Journal des Tribunaux*, 1992, pp. 305-309.

the legality requirement (is there a law?)[96]. When they *have* to consider the "necessity" requirement, they replace it by the more flexible proportionality test. This is regrettable because there is a structural lack of information about the notion of the democratic state, which should be filled out precisely by the legislature and the judges. Assertions such as "we must defend our democracy against terrorism" give the impression that democracy is a kind of substance existing in itself. We never get to know what this substance is, but we are permanently invited and tempted to accept the proposition that we have to defend this democracy by all means, even undemocratic ones[97]. This is dangerous. Democracy is no substance but a whole of practices and processes that we associate with the label "democratic". It consists of a permanent questioning of all the practices and processes which make a society democratic. The core of constitutional thinking is to participate in that questioning by focussing upon some values that are considered to be fundamental.

## 6 COMBINING PRIVACY AND DATA PROTECTION

### 6.1 Combining the tools

In the preceding pages we critically discussed the shift from opacity towards transparency in European human rights law. There are numerous ways to revitalise or to protect the proper function of privacy and to make it relevant again for framing law enforcement.

On the level of case law, privacy could regain something of its esteem if the judges of the European Court of Human Rights would stop focusing only upon the legality criterion (if a statute makes everything possible, human rights are threatened and not protected) and start again taking the "necessary in a democratic society" test seriously: judges in a constitutional court have a crucial political role to play in drawing the line between acceptable and non-acceptable power, setting the switch between opacity tools and transparency tools.

96 Cf. I. Cameron, *o.c.*, p. 35.

97 J. BLOMMAERT, "Veiligheid en democratie?" [Security or Democracy?], in Liga voor Mensenrechten (editor), *Wordt de Europese ruimte van vrijheid, veiligheid en rechtvaardigheid een politiestaat?*, Gent, Liga voor Mensenrechten, 2003, (67-70), 67.

Maybe one day a legal culture will be firmly established in which it is regarded as self evident that interference with the individual citizen by the state requires an explicit basis in law, even in common law systems that have taken the opposite view in the past[98]. Hence, one can expect a future rich with cases in which the focus is on the requirement of "necessity in a democratic society"[99].

On the level of the legislator more attention should be paid to the distinct nature of the two sorts of legal tools that were invented to cope with power in a democratic constitutional state: the opacity tools establishing the limits of interferences in an individual's life by public and private powers on the one hand, and the transparency tools channelling and regulating the legitimate use of power on the other hand. Ideally, every time the legislator acted he would consider both tools and identify the kind of tool necessary for a given problem. How much of which tool is necessary when? Each tool supplements and pre-suppose the other. Channelling power in the mist is doomed to fail; limits and points of departure are necessary. Approaching new phenomena and new possibilities for law enforcement with heavy prohibitions may circumvent the legitimate interest of the state or block potentially interesting developments *e.g.* with regard to the use of new technology[100]. It may also lead to a situation in which the prohibitions are not respected. This would leave power relations uncontrolled, due to the lack of tools. Hence, an approach based mainly on opacity tools should be considered with due care.

If no specific action is taken towards new police or private demands to use new technological means, in a European context, data protection will apply. This would however imply, due to the enabling logic of this legal framework, that we say "yes" to all new forms of power applications,

98 P. ALLDRIGDE & CH. BRANTS, *l.c.*, 13.

99 Case law such as the *Khan* judgement, refusing to apply the principle that illegaly obtained privacy evidence should be rejected, seems to contradict this view of the future. By weakening the importance of privacy, privacy will lose its capacity as an opacity tool. The *Khan* doctrine (followed in cases such as *Doerga v. the Netherlands* and *P. G. and J. H. v. The United Kingdom*) is discussed in P. DE HERT, "De soevereiniteit van de mensenrechten: aantasting door de uitlevering en het bewijsrecht" [Sovereignity of human rights: threats created by the law of extradition and by the law of evidence], *Panopticon*, *Tijdschrift voor strafrecht, criminologie en forensisch welzijnswerk*, 2004, v. 25, n. 3, 229-238 and in P. DE HERT & F. P. ÖLCER, "Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging" [The notion of privacy made innocent. Implications for criminal procedure], *Strafblad. Het nieuwe tijdschrift voor strafrecht*, 2004, v. 2, n. 2, pp. 115-134

100 This approach is followed *e.g.* in Article 13 of the Charter of fundamental rights of European Union of 7 December 2000 prohibiting "eugenic practices" in particular those aiming at the selection of persons and in "making the human body and its parts a source of financial gain".

even when their legitimate character can be disputed. Also, data protection legislation tends to be very difficult and technical. This may give way to erosion and a denial of this new area of law. The strength of data protection, however, is not to be neglected. *The complex question "is this a privacy issue?" is replaced by a more neutral and objective question "are personal data processed?".* Data protection, as such, is a general framework for all kinds of surveillance: the written word, sounds, images, DNA and even smells can be understood as personal data falling under the scope of data protection. For instance, in the case of closed circuit TV (CCTV) – a technology that can be legally installed and operated, but very easily abused and used for unlawful purposes (for example by turning the camera away from the machines and towards the working personnel) – the attention of data protection for all processing aspects (from collection to destruction) is a guarantee. Moreover, data protection brings the issue of consent and the waiver of rights into focus, by making it explicitly possible in some cases (but not all), and only under specific conditions. We don't see how privacy case law could form an alternative for the elaborate list of rights and duties foreseen by the data protection bills. (How many cases and how many precedents are needed to achieve the same results?).

Furthermore, it should be stressed that the two approaches do not exclude each other. They depend on policy choices, which can be revised and adapted. As a result, pursuit of the transparency approach (regulating instead of prohibiting) might after some time and practice show that the opacity approach is preferable (or vice versa) or that a better balance between the two approaches should be devised. In reality one will rarely find legal solutions based exclusively upon one tool. A blend of the two approaches will generally be preferable, since a solid legal framework should be both flexible (transparency) and firmly anchored in intelligible normative choices (opacity). A good example of such balancing of approaches is given in Directive 2002/58/EC on privacy and electronic communications of 12 July 2002 (supra). This Directive puts an end to the long-lasting controversy regarding direct marketing by explicitly adopting an opt-in system which inherently implies the prohibition of unsolicited marketing mail unless the user makes an explicit request to receive it. In this example it becomes clear how the model of channelling business practices (transparency) is supplemented by the limiting model of a negative obligation (opacity) after due consideration and debate. A second example can be found in national legislations dealing with CCTV, containing for instance prohibitions on

directing cameras towards the entrances of private premises. A third example is provided by the numerous national bills on the use of DNA--samples in criminal matters. Although the processing of DNA-samples, from the perspective of data protection (Directive no. 95/46/EC), is in fact an ordinary application of processing of personal data, the riskiness of the matter explains why states supplement general data protection bills with specific prohibitive bills on DNA.

Of course our approach raises the question of the criteria for the application of the distinct tools to the (new) developments and techniques. When will opacity (privacy) be called upon, when will transparency (data protection) apply? Such criteria and norms should be used to set the switch between a privacy-opacity approach (prohibitive rules that limit power) and a data protection-transparency approach (regulations that channel power). Especially when faced with new problems, such as the insistence on security (of various government initiatives) or the development of new technologies, the approach should consist in combining the tools appropriately. The issue of the criteria is crucial because it will determine the sort of legal measures that will be taken and applied. The differences are sensible. On the one hand, legal measures from the privacy/opacity perspective include the elaboration (and strengthening) of prohibitionary legal regimes and protect and enforce the anonymity of behaviour (*e.g.* through approving regulations of techniques of anonymity, pseudonymity, identity management, [...]). On the other hand, legal measures from the data protection/transparency perspective are directed towards the data controllers allowing "to watch the watchdogs".

With regard to new technologies, the (European) legislator will have to assess the risks and threats to individual liberty separately[101]. The two complementary instruments at his disposal allow for a well-balanced regulatory framework. It can be assumed that there will be reliance on data protection and other transparency tools by default and that only in rare cases or after due consideration of actual risks will prohibitive opacity measures be taken to protect rights and freedoms and to promote trust in the Information Society. The sheer fact that both instruments co-exist implies a permanent determination to assess the level of acceptance and implementation of use

101 Anyhow, in dealing with future technologies with still unknown potential and bearing risks for the liberty of the individual, we should adopt a *precautionary* approach (a process that includes information gathering, broad consultation, participative procedures of decision-making, etc.).

and potential abuse of new technologies and the ensuing enforcement of legal rules. This process may explain why factors such as September 11 and new technological developments can account for a shift from transparency tools to opacity tools (when trust is fragile) or vice versa (when trust is reestablished).

### 6.2 Determining the switch

The importance of the issue of determining the criteria for the handling of the switch leading to a policy of opacity or transparency cannot be underestimated. Of course the choices concerning these criteria will be made by the legislators, preferably after a large and informed societal debate amongst the totality of those concerned (business, government, citizens, civil liberties groups, privacy advocates, [...]) and by competent judges at national and international level. For our part, we can only deal with the question of the criteria from a prospective, exploratory and modest point of view. As academic researchers we can and must do "no more" than to propose and suggest the concepts, tools and paths that we can derive from our research and reflection.

What should be protected through opacity or privacy tools and what should be protected through transparency tools? What is, in a democratic constitutional society, so essential that it must be as a rule shielded from interference by others (public and private actors)? Which aspects of individual life in an open society must be protected against openness and transparency?[102] Which aspects of individual life should be withdrawn from scrutiny, surveillance and control? Where are hard norms needed? Where should ad hoc balancing be replaced by categorical balancing?

102 This is actually the core question of David Brin's inspiring book D. BRIN, *o.c.*, 378 p. Nonetheless, we defend a different position, inasmuch as we do not carry *mutual transparency* (and *symmetric information flows*) as far as Brin does. We do not value anonymity and opacity so negatively as he does. The fundamental reason for this, we think, is that Brin distinguishes freedom ("personal sovereignty") and privacy much more sharply than we do: for him privacy is "a delicacy that free people can pour for themselves as much or as little as they choose [...] Privacy is a wonderful highly desirable *benefit* of freedom" (p. 79). Brin associates freedom with free speech and comes to the conclusion that "there can be few compromises when it comes to the underpinnings of liberty. Without both individual freedom and distributed sovereignty, all our vaunted modern privacy would vanish into legend" (p. 79). Our understanding of privacy is precisely interwoven with the "underpinnings of liberty", and that is why we tend to give privacy a more positive and broader connotation. For Brin, privacy only concerns a limited array of aspects which come close to the sanctity of the home: "[...] I won't exchange my liberty or anyone else's – for security. I certainly won't give up essential privacy: of home, hearth, and the intimacy that one shares with just a few".

The answers to these questions must be formulated by reference to the basic features of the democratic constitutional state. From this perspective opacity/privacy rules – prohibitionary rules – should guarantee those aspects of an individual's life that embody the conditions for his/her autonomy (or self-determination, or freedom, or "personal sovereignty"). This is the case because it is precisely this autonomy that develops and fuels both one's participation in the civil and political life and the fact that one develops a personality and a social/relational life. Privacy must protect what lies behind the persona, the mask that makes an individual a legal person (cf. anonymity). It must preserve the roots of individual autonomy against outside steering, against disproportionate power balances, precisely because such interference and unbalanced power relations do more than threaten individual freedom; they also threaten the very nature of our societies. Privacy and opacity are needed because, as we have already explained, a democratic constitutional state is primarily concerned with the protection of the individuals' autonomy (and resistance) in vertical, but also in horizontal power relations.

### 6.3 An example: camera surveillance

Both in Europe and in the United States there is evidence of a common understanding of the impropriety of filming people in private houses. In the early seventies, abuses with spy devices gave way to specific criminal laws on visual intrusion in Italy, the Netherlands and France[103]. Filming what happens inside houses was targeted by very simple, clear-cut prohibitions. On this solid basis, a data protection framework was build to organise protection for people under surveillance in the public space. In 1995, France enacted a much broader bill initiating a system of CCTV-rights and duties, whereby use of CCTV without prior notification to a control board is a criminal deed, as is refusing access to the images and refusing rights of correction and rectification[104]. Due to data protection, countries with older specific criminal bills, such as France, are now able to redefine their scope of protection. In some German Länder specific video-clauses are introduced in local data protection bills. The Schleswig-Holstein bill allows

103 Cf. section 4 of the Italian act respecting workers' freedom of 20 may 1970 (amended in 1990); the French law of 17 July 1970 (article 368 (old) penal code/article 226 new penal code); the Dutch law of 7 April 1971 (art. 139f-g, 372-375 and 441a penal code).

104 Bill n. 95-73 "d'orientation et de programmation relative à la sécurité", 21 January 1995; P. DE HERT, "La police française en l'an 2000", *Politeia. Revue professionnelle Belge des services de police*, 1995, n. 4, pp. 12-16.

EVS of public places when this is necessary for the protection of the premises and when other legitimate interests of a higher rank are not present. In the case of recordings of visual data, there has to be a warning to alert the people concerned[105].

Belgium has a general bill on data protection, but did not and does not have a bill on digital video surveillance or video surveillance. In 1994 the Minister of Justice refused to enact specific legislation with simple prohibitions on certain uses of CCTV because he thought this would inhibit the legitimate business of CCTV, deemed necessary for safety purposes[106]. When, subsequently, the Belgian data protection authority drafted recommendations for the use of CCTV based on the 1992 bill on data protection, it reinvented or imported the French or Dutch "very simple" prohibitions on filming private spaces, without however referring to these prohibitions[107].

This example shows that data protection bills and criminal or other prohibitions do not contradict each other, but have a complementary nature. Different domains of law have different kinds of logic that can be combined, in this case criminal law (prohibitive logic) and data protection (channelling logic). Where law is an appropriate and effective instrument, there is a need to identify the relevant harm with precision in order to craft a precise and targeted solution, capable of carrying basic messages that bring "ontological security" (cf. above). We thus favour a framework that weighs the benefits of different kinds of legal logics against the possible threats to privacy. Using this balancing approach, we advocate narrowly targeted legislation aimed at enhancing the protection of sensitive domains of human life (for instance, processing of medical and financial information). The core of privacy should be clearly defined in terms of harmful uses. Normal processing of data and potential harms must be addressed by data protection with its channelling/procedural logic[108].

Depending on the circumstances, the existing equilibrium between the use of tools of opacity and the use of tools of transparency has to be

105 Cf. section 32 of the Schleswig-Holstein bill "zum Schutz personenbezogener informationen", 30 October 1991.

106 See in detail P. DE HERT, O. DE SCHUTTER & S. GUTWIRTH, "Pour une réglementation de la vidéosurveillance" [Plea for a legal framework for CCTV], *Journal des tribunaux*, 21 September 1996, pp. 569-579.

107 *Ibid.*

108 L. BERGKAMP, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy", *Computer Law and Security Report*, 2002, v. 18, n. 1, p. 46.

altered. A fine example is provided by a recent bill in Holland on video monitoring of employees, which prohibits the secret use of a camera to detect fraud, except by the police. This prohibition, which supplements existing prohibitions on filming of private premises and existing rules of data protection governing other use of CCTV, effectively forbids the installation of a hidden camera by a shop-keeper who suspects that an employee is stealing. The new prohibition contains one clear message: from now on, the shopkeeper will have to ask the police to mount such surveillance[109].

### 6.4 A second example: passenger profiling

In a recent Dutch publication we have carried out a similar exercise with regard to the Computer Assisted Passenger Pre-Screening System (CAPPS II)[110]. We recall that the core idea of this U.S. project is to focus security resources on suspicious travellers, while ensuring that most people are not inconvenienced by this heightened security. The aim of the American initiative is to screen risks before boarding. CAPPS-II is designed to reduce the number of people for further screening and is intended to "restore public trust" in airline travel. It proposes to use extensive data mining of credit history, criminal records, travel patterns and to expand the range of databases searched for suspicious activities to profile *all* airline passengers. The new system uses an algorithm to determine indicators of characteristics or behaviour patterns that are related to the occurrence of certain behaviour. Risk scores then help to determine whether a passenger can board a flight. CAPPS-II allows airport authorities to discover through a computer search whether a person is to be identified as a possible suspect. The information is forwarded to the appropriate law enforcement agencies. Before boarding the plane, passengers are assigned one of three rankings printed in code on their boarding passes: green requires routine security, yellow, "added checks", while red bars passengers from flying and subjects them to law enforcement

109 THIERRY D. M., "Het gebruik van camera's ter opsporing van strafbare feiten op de werkvloer", *Bb* 24 juni 2001, n. 12, pp. 132-134.

110 P. DE HERT & S. GUTWIRTH, "Veiligheid en grondrechten. Het belang van een evenwichtige privacypolitiek" [Security and Human Rights. The Importance of a Balanced Privacy Policy], in E. R. MULLER (red.), *Veiligheid. Studies over inhoud, organisatie en maatregelen*, Alphen aan den Rijn, Kluwer, 2004, 585-630. See also M. V. PÉREZ ASINARI & Y. POULLET, "The Airline Passenger Data Disclosure Case and the EU-US Debate", *Computer Law & Security Report*, 2004, v. 20, n. 2; 98-116; M. V. PÉREZ ASINARI & Y. POULLET, "Airline Passengers" Data: Adoption of an Adequacy Decision by the European Commission. How will the Story End?", *Computer Law & Security Report*, 2004, v. 20, n. 5, 370-376.

investigation. The red code would be reserved for those on terrorist watch lists.

The CAPPS-II initiative has consequences for Europe. At least since 5 march 2003, United States authorities have had access to most European airlines" passenger databases. An agreement between the European Commission and United States Customs gives the USA online access to the passenger name record (PNR) data of all Europe-based airline carriers for flights that go to, from or through the USA. The scope of the agreement is wide. The agreement says that "Customs will retain the data no longer than is required for the purpose for which it was stored". But at the same time it is clear that the data is stored for an almost unlimited number of purposes, certainly not limited to fighting terrorism: "PNR data is used by Customs strictly for enforcement purposes, including use in threat analysis to identify and interdict potential terrorists and other threats to national and public security". The U.S. Customs will also share the data with all other U.S. agencies: "Other law enforcement entities may specifically request PNR information from Customs and Customs, in its discretion, may provide such information for national security or in furtherance of other legitimate law enforcement purposes"[111]. The agreement reads as an assurance that EU passenger data will be stored in FBI, NSA and CIA databases.

The agreement between the European Commission and U.S. authorities on the transmission of PNR data has encountered fierce opposition during a public hearing at the European parliament. During a public hearing on 25 March 2003in the European parliament the Commission argued that it had no choice but to accept the U.S. demands for passenger data. Threats to fine European airlines or even halt landing rights were taken very seriously by the Commission. But many participants were not satisfied with the explanation that the Commission had been blackmailed and couldn't do anything about it. They argued that the transfer of PNR data has no legal basis and is a direct violation of the EU Data Protection Directive. The European Parliament decided, in a unique move, to bring the case before the European Court of Justice. A judgement is expected in 2005.

Our contribution to the debate has been to identify some structural shortcomings in the European responses. Fundamentally, events have

111 European Commission/US Customs talk on Passenger Name Record (PNR) transmission, *Joint Statement of 17/18 February 2003*, see http://europa.eu.int/comm/external_relations/us/intro/pnrjoint03_1702.htm.

proven the limited reach of data protection. Europe applied transparency tools where opacity-like answers were needed. Data protection authorities drew attention very early to the problematic nature of the initiative, but were unable to bring the case to a satisfactory end. The fundamental question was circumvented, namely: do we want these kind of data-mining practices in Europe with all the risks for citizens who match a profile? Politicians, not surprisingly, had to take over and phrase the debate in these elementary terms. Unable to per suade the European Commission to adopt a firm position, they finally referred the matter to the European Court of Justice. We can only hope that this Court will effectively deal with the crucial issue, viz. the desirability or necessity of these projects for modern democratic states. It might very well be that the outcome will be a positive "go" and then data protection can do its proper job and clean up the more procedural problems with the American project.

### 6.5 Workable criteria?

It is possible for us to be more specific about the use of the respective tools or do we abdicate? When are opacity tools necessary? Only a beginning of the answer is possible.

Firstly, we think that opacity tools might be needed with respect to the set of values protected through the inviolability or sanctity of the home. People need places were they can rest and come to terms with themselves in a sphere of trust and security, in an environment where they experience "ontological security" – a place where family life is possible. Such places represent a private territory, a sanctuary; they imply intimacy, anonymity and a possibility of solitude. The protection of the home is one of the oldest human rights and nowadays it is still enshrined in international human rights law and in national constitutions. For these legislations home is where the house is, or by extension, the car, the caravan, [...] Their terms refer to the material/physical home. But, indeed, "being at home" means more than being in a certain physical environment, it means also feeling at ease, comfortable. In French the concept of "home" can also be translated by *chez soi* which is actually expressive from our point of view. It is the *chez soi* that a democratic constitutional state respects and values (contrary to totalitarian states): the idea that one can be with him/herself without outside interference in order to "manage" his/her relational, civil and political life as a free being. In a certain sense it is precisely this *chez soi* that lies protected behind the mask of legal personality. Values protected by the inviolability

of the home therefore might thus also need protection outside the material house, and especially in the "virtual world".

Secondly, tools of a prohibitive nature are obviously required when other firmly rooted (in tradition or in law) human rights are at stake, such as the right to have correspondence and the content of communication protected (cf. *supra*). Disregard of these rights has brought legislation in the United Kingdom giving the employer almost absolute discretion to monitor destinations and control of e-mail sent by employees[112]. This stands in complete contrast with the approach followed in Belgium, where concerns about the right to have correspondence respected has inspired a regulation whereby the employer can check on the destination and on other data about the telecommunication, but cannot check on the content of the communication[113].

Thirdly, opacity exist within the framework of data protection, *e.g.* in the case of sensible data or in the case of decisions regarding individuals taken solely on the basis of automatic profiling. Indeed, the additional danger here is linked to possible discriminatory effects of such practices.

Fourthly, a need for opacity can be drawn from the function of human rights in promoting and encouraging citizenship. When certain law enforcement tactics threaten aspects of human behaviour vital to the formation of the free and equal citizen, a prohibitive logic will impose itself.

Finally, opacity tools can be implemented when there is a societal interest in ending ongoing debates and a need to enhance legal certainty.

Having tentatively set out some touchstones which we deem to be relevant for identifying issues that demand a privacy/opacity legal approach, it is easier to point out what, at the other side of the switch, will fall under the data protection/transparency legal approach. We are tempted to answer: in principle, all forms of processing of personal data that do not demand categorical balancing by the (constitutional) legislator on the basis of the guidelines identified above. In reality this residual category may well have a considerable dimension, especially in horizontal relations where the

112 K. BEST & R. MCCUSKER, "The Scrutiny of the Electronic Communications of Businesses: Striking the Balance Between the Power to Intercept and the Right to Privacy?", *Web Journal of Current Legal Issues*, 2002/1, via http://webjcli.ncl.ac.uk/2002/issue1/kb-rm1.html, pp. 9-11.

113 P. DE HERT, "C.A.O. n. 81 en advies n. 10/2000 over controle van Internet en e-mail" [Labour law: Soft law on e-mail and Internet practices], *Rechtskundig weekblad,* 2002-2003, v. 66/33 (19 April 2003), pp. 1281-1294.

existence of unequal power relations should not be taken as a starting point. In all cases where consent (still) plays an important role, it can be assumed that the guidelines for the opacity approach are not met. Individual responsibility, consent and ad hoc balancing are sufficient but indispensable conditions for meeting the requirements of a constitutional state. Correlatively, this implies that secret processing of personal data must be prohibited, since this secret or unknown character renders the mise en oeuvre of transparency tools or data protection impossible. Informed consent is a *conditio sine qua non* for subsequent controls on data processing[114]. There is little room for a policy based on the full liberty of processing data. Transparency tools are the default tools in all areas of data processing. Because this processing of data is always intertwined with power relationships[115], a democratic constitutional state must foresee rules that permit to channel this power, namely rules of transparency and accountability, viz. data protection rules.

## CONCLUSION

The development of the democratic constitutional state has led to the invention and elaboration of two complementary sorts of legal tools, namely normative opacity tools that draw the limits of interference with individuals, and transparency tools that organise the channelling, control and restraint of power. Privacy is an example of the former, data protection and criminal procedure are mainly examples of the latter. Hence, privacy is about much more than just accountability and foreseeability. This is the reason why case-law and literature, in our opinion, tend to overstress the importance of accountability and foreseeability relating to privacy limitations to the detriment of the normative and prohibitive drawing of barriers. There is too much "yes, if" and a lack of "no". By recognising human rights, the democratic constitutional state generated legal mechanisms to impose non-interference in the private sphere. In our opinion, privacy is closely linked to this endeavour as it tends to protect the values of liberty by erecting a legal shield against interferences. More concretely this shield can take the form of (legal) claims of immunity, anonymity, pseudonymity, opacity and sanctity.

114 Cf. The fairness principle of the OECD guidelines and Treaty 108.

115 Why? Because the processing of information about individuals always opens the door to some form of control. Because it intimidates. Because people adapt their behaviour if it is clear that information is gathered. This is not intrinsically a "bad thing", but just a fact that must be taken seriously into account.

This normative position is echoed in the legal landscape. The right to privacy is a widely recognised opacity tool to prohibit certain uses of power. It may not be the strongest human right listed in the ECHR and it may well also be that the "reign" of privacy in discourse is over, but nevertheless the right is there and it has its proper place, a quintessential place. The interpretative work of the European Court on Human Rights is ambiguous. Obviously, the European judges prefer to concentrate on non-privacy issues such as accountability and foreseeability of privacy limitations. Gradually the Court has developed the view that a legal basis for privacy infringements should not only exist, but should also meet some qualitative requirements, namely accessibility and foreseeability. Also the Court has fused in its analysis elements borrowed from procedural rights enshrined in other provisions of the Convention. But the question whether a certain practice is "necessary in a democratic society" is often not addressed by the Court when a breach of the legality requirement is found. Constitutional reasonableness encompasses substantive fairness *and* procedural regularity and the two are often tightly intertwined, but in a sensible division of constitutional labour these issues are best treated separately on their own merits. Searches with a maximum of procedural guarantees might well be unreasonable in the light of Article 8, when they allow for an unwanted concentration of power (the idea behind opacity tools). On the other hand it is clearly possible to conceive privacy infringements without procedural guarantees that are nevertheless reasonable, for instance metal detectors at airports[116]. Elaborating codes of criminal procedure, for instance, with regard to telephone tapping, is not a command that follows from Article 8.

From that perspective the constitutionalisation of the right to data protection in the EU Charter represents a positive evolution, for data protection has a precise target which is distinct from privacy concerns and aims at organising the fair processing of personal data by both public and private actors. That is why the precise requirements imposed upon the processing of personal data have been developed by data protection law and not by the constitutional construction of privacy. Moreover, due to its channelling logic data protection allows for a sensible constitutional division of labour. Its recognition may pave the way for a rediscovery of the power blocking nature of the privacy right. Privacy and data protection

116 A. R. AMAR, *The Constitution and Criminal Procedure. First Principles*, New Haven and London, Yale U.P., 1997, pp. 38-39.

supplement each other and pre-suppose each other. We have suggested that the European legislator considers both tools and uses them accordingly. By giving concrete examples (*e.g.* video surveillance and CAPPS-II) and by identifying guidelines for switching from the privacy logic to the data protection logic and back, this contribution aims at illuminating how Europe is *and* should be dealing with challenges created by new power demands, especially in the field of law enforcement.

Privacy functions as a tool to distinguish between the reasonable and the unreasonable and to stop law enforcement power whenever it crosses a normative line. Privacy is not a tool to regulate reasonable law enforcement power by devising mechanisms of transparency, control and accountability. Opacity and transparency each have their own role to play. They are not communicating vessels. Hence, unlike Etzioni, we do not think that public authorities cannot be denied technologies and means for crime fighting if their implementation is linked to enough transparency and accountability[117]. On the contrary, privacy implies the making normative choices: some intrusions are just too threatening for the fundamentals of the democratic constitutional state to be accepted even under a stringent regime of accountability. Other intrusions, however, will be felt to be acceptable and necessary in the light of other sometimes predominating interests. Only then, after such a normative weighing of privacy and other interests, privacy invasive and liberty threatening measures can be, exceptionally and regrettably, accepted and submitted to the legal conditions of transparency and accountability.

117 A. ETZIONI, "Implications of Select New Technologies for Individual Rights and Public Safety", *Harvard Journal of Law & Technology*, 2002, v. 15, n. 2, p. 34: "If accountability is deficient, the remedy is to adjust accountability, not to deny the measure altogether".

**Sobre os autores:**

**Serge Gutwirth** | *E-mail:* serge.gutwirth@vub.ac.be

Professor at the Faculty of Law and Criminology of the VUB, where he studied law, criminology and also obtained a post-graduate degree in technology and science studies. Today he is mainly focussing on the difficult articulations between law, politics, technology and ethics with regards to concrete emerging issues (*e.g.* data protection, S&M, gene editing, [...]). Since 2017 he started doing research on the resurgence of the commons. In 1999 Gutwirth has founded the VUB-Research group on human rights (HUMR), which he chaired until 2003, after which his colleague Paul De Hert took over. After obtaining the fellowship in October 2003 he founded the VUB-Research group Law Science Technology & Society (LSTS) which still (co-)chairs. Today, with more than 30 researchers at all levels of experience, LSTS has become a prominent European research institute. Next to thisGutwirth has been Vice-Dean of the Faculty (2012-2018), Vice Chair of the VUB's Research Council from 2002 to 2013, (co-)Director of LSTS (2003-[...]) and Chair of the Department of Interdisciplinary Studies of the law (JURI) from October 2018 on.

**Paul De Hert** | *E-mail:* pdehert@law.leidenuniv.nl

Prof. Paul De Hert's work addresses problems in the area of privacy & technology, human rights and criminal law. A human rights approach combined with a concern for theory is the common denominator of all his work. In his formative years, De Hert studied law, philosophy and religious sciences (1985-1992). He is Director of the Research group on human rights (FRC) and Vice-Dean of the Faculty and former Director of the Research group Law Science Technology & Society (LSTS), and of the Department of Interdisciplinary Studies of Law.He is board member of several Belgian, Dutch and (other) international scientific journals such as The Computer Law & Security Review (Elsevier), The Inter-American and European Human Rights Journal (Intersentia) and Criminal Law & Philosophy (Springer). He is co-editor in chief of the Supranational Criminal Law Series (Intersentia) and the New Journal of European Criminal law (Sage). Since 2008 he has edited with Serge Gutwirth, Ronald Leenes and others annual books on data protection law (before Springer, now Hart) that, – judging sales numbers, quotations and downloads, attack a massive readership and have contributed to creating the legal, academic discipline of data protection law. De Hert is now series editor of The Computers, Privacy and Data Protection series, now published by Hart.

Artigo convidado.