Biometrics between opacity and transparency

Serge Gutwirth
Law Science Technology & Society (LSTS)
Department of Metajuridica, Faculty of Law, Brussels, Belgium

Summary. The overall aim of the democratic constitutional state is to protect a social order in which the individual liberty of the citizen is a major concern. As a consequence the democratic constitutional state should guarantee simultaneously and paradoxically a high level of individual freedom and an order in which such freedom is made possible and guaranteed. Biometrics provide a strong and expressive example both of the necessity to address the issue of opacity and transparency and the complexity of the process. Indeed, the large scale use of biometrics does not only question the position of the individual in society, but it also alters the architecture or nature of this society as such.

Key words: privacy, data protection, biometrics, democracy.

Riassunto *(Biometria tra opacità e trasparenza)*. Lo scopo generale di ogni stato democratico costituzionale è proteggere un ordine sociale in cui la libertà di ogni cittadino costituisce una cura precipua. Di conseguenza uno stato democratico costituzionale dovrebbe garantire simultaneamente e paradossalmente un livello elevato di libertà individuale e un ordine in cui tale libertà è permessa ed è garantita. La biometria fornisce un esempio efficace e significativo della necessità di affrontare opacità e trasparenze e anche in generale la complessità di questo processo. Effettivamente, l'uso su grande scala della biometria non solo mette in discussione la posizione dell'individuo nella società, ma altera l'architettura e la stessa natura della nostra società in quanto tale.

Parole chiave: privacy, protezione dei dati, biometria, democrazia.

INTRODUCTION

In this short contribution I would like to present some thoughts from the perspective of law and legal theory. These thoughts tend to draw a distinction that may provide a useful conceptual background for the discussion on biometrics.

If we challenge to think about biometrics not only from an instrumental point of view "what can biometrics do?", but also from a normative perspective "what should we – ethically, socially, legally – accept they would do?", this implies that the use of biometrics should be weighed against the fundamental principles of a democratic constitutional state.

In one sentence one might say that the overall aim of the democratic constitutional state is to protect a social order in which the individual liberty of the citizen is a major concern. As a consequence the democratic constitutional state should guarantee simultaneously and paradoxically a high level of individual freedom *and* an order in which such freedom is made possible and guaranteed.

As a result of this *double bind* the democratic constitutional state is constantly under tension because the individual liberties must be tuned to a social order, which, in its turn, is precisely devised to be constitutive for the liberty of its individual participants. Hence the democratic constitutional state is not a static order, but it is a dynamic one, which evolves as a result of a permanent balancing of individual, social and state interests and concerns. Both a private and a public sphere must be constituted and tuned.

The history and practice of democratic constitutional states (both at national and at subnational or supranational level) has shown that such states always have elaborated two complementary sorts of legal or constitutional tools, which Paul De Hert and I have called opacity tools and transparency tools [1, 2]. These tools offer legislators the possibility to translate fundamentally different policy choices into legislation. From this perspective both tools are a part of the means by which a democratic constitutional state can dynamically organise the relations between individual, social and state concerns and interests.

OPACITY AND TRANSPARENCY TOOLS

Opacity tools are legal tools/measures that protect individuals and their liberty/autonomy against state interventions and against private actors: they guarantee the non-interference in individual matters, they work as shields or bulwarks. Such tools are of course closely interwoven with the recognition of human rights and a sphere of individual autono-

Indirizzo per la corrispondenza (Address for correspondence): Serge Gutwirth, Law Science Technology & Society (LSTS) Department of Metajuridica, Faculty of Law, Vrije Universiteit Brussels, Pleinlaan 2 Building B, B-1050 Brussels Belgium. E-mail: serge.gutwirth@vub.ac.be

my and self-determination. Indeed, by recognizing "first generation" human rights, the liberal revolutions of the 17th-18th centuries in England, the US and France have laid the foundations for the (legal) distinction and enforcement of the public and private spheres. 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.

Opacity tools, thus, are legal tools that enact a prohibition to interfere with the individual's autonomy and accordingly impose a hands-off or abstention policy from the state and private actors (as a result of the "horizontal effect" of human rights, for example). In other words, it can be said that they enforce the anonymity of behaviour in our societies. Opacity tools set *limits* to the interference of the power with the individuals' autonomy, and as such, they have a strong *normative nature*. The regime they install is that of a principled proscription: they foresee "no, but …-law". 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, autonomy and identity-building: some actions are considered unlawful even if the individual consents. A good example is article 3 of the Charter of fundamental rights of European Union which prohibits "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".

Another example of an opacity tool is the protection of the "sanctity" or inviolability of the home, which indeed properly expresses the concern for the respect of the individual's autonomy: the public authorities (but also the other citizens) must respect the bounds of the home. A home is inviolable, and a breach of that principle generally engenders criminal prosecution. Once inside a home, people are more free from interference from the government (and others) than outside. A home is a privileged setting. This doesn't 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. 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 the police and judicial authorities is strictly regulated.

It should be added that opacity tools, such as the protection of privacy, are not exclusively characterised by the negative function of shielding and protecting the individual against interferences. Such a preservation also has an important positive function for it is simultaneously a condition for his/her free and unbiased participation in the political processes of the democratic constitutional state. Hence opacity tools are protecting both negative and positive freedom: on the one hand they work as shields against interferences in individual matters, but on the other, and simultaneously, they provide the solid ground for a succesful a public sphere in which the democratic political life can take form.

Transparency tools are very different: they are mainly regulatory. Although their objective is (also) to control state (and other) powers, they do not proceed by drawing the boundaries of power's reach. On the contrary transparency tools tend to regulate accepted exercise of power. Transparency tools are not prohibitive, but aim at channelling, regulating and controlling legitimate powers: they affect the way power can be exercised, they make the use of power legitimate. More concretely, transparency tools provide means of control of power by the citizens, controlling bodies or organisations, and by the other state powers. Thus: transparency tools intend to compel government and private actors to "good practices" by focusing on the transparency of governmental or private decision-making, which is indeed the primary condition for an accountable and responsible form of governance. They define the principles by which the state and private actors must organise their conduct in relation to citizens. In other words, transparency tools tend to make the powerful transparent and accountable: they allow us "to watch the watchdogs". Transparency tools install a regime of conditional acceptance: they foresee "yes, but …-law". A good example is administrative law, which regulates the modalities of the executive power and ensures accountability by governmental actors.

The origin of transparency tools lies with the principles of the rule of law and constitutionalism. On the one hand, the principle of legality of government foresees 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. This implies the important fact that the government is accountable and that its actions must be controllable, and thus transparent. On the other hand, the trias politica or, in other words, the system of balancing of powers aims at limiting state power 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 and pluricentric system of mutual control or "checks and balances". Such a system implies the mutual accountability of state powers, and thus again, their reciprocal transparency and controllability.

To summarise the distinctions it can hence be said that:

- opacity tools embody normative choices about the limits of power while transparency tools aim at the control and channelling of legitimate or already normatively accepted power; while the latter are thus directed towards legitimate uses of power, the former are indicating where power should not come (protecting the citizens against illegitimate and excessive uses of power);
- opacity tools are determining what is in principle out of bounds "no, but …", hence, what is deemed

so essentially individual that it must be shielded against interferences while transparency tools regulate exercise of power "yes, but …" take into account that the temptations of abuse of power are huge and empower the citizens and special watchdogs to have an eye on the legitimate use of power: they put counter powers into place. On the opacity side there is a prohibition rule which is generally, but not always (*e.g.*, the prohibition of torture) subject to exceptions; on the transparency side there is a regulated acceptance. If we would apply the concepts to surveillance, the opacity approach would entail a prohibition of surveillance and imply a right not to be surveilled, while the transparency approach would regulate accepted surveillance and imply a right not to be under unregulated surveillance [3].

Opacity and transparency tools belong to the same constitutional architecture. They were conceived simultaneously, at the historical moment of the conceptual birth of the democratic constitutional state, both with the aim of contributing to the control of power. They are complementary. One could say that they are linked by a switch: leaving the opacity of the individual means stepping over onto a system of transparency of power. The way both tools are articulated will determine how much non-interference or negative freedom an individual can expect and will be enabled to claim. Such balance between an opaque and autonomous individual sphere and legitimate interventions of the state and private players, is indeed crucial for establishing the type of government in a society. The complex search for the appropriate combination between both tools is a permanently challenging issue for parliaments and policy-makers.

PRIVACY AND DATA PROTECTION

The differences between the two tools appear very clearly if one looks at the articles 7 and 8 of the Charter of Fundamental Rights of the European Union (included in the draft Constitution). These articles respectively pertain to privacy and data protection:

Article 7: "Everyone has the right to respect for his or her private and family life, home and communications".

Article 8: "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".

Art. 7 provides a good example of an opacity tool because it limits the possible interferences with the individuals' private and family life, home and communications. In a more generic way it can be said that this article protects the individuals' privacy. It is normative and prohibitive, but, of course, the prohibition is not absolute. The rule is a "no", but exceptions are thinkable under a number of conditions. In fact, art. 7 of the Charter is a reproduction of the first paragraph of art. 8 of the European Convention on Human Rights, which in its second paragraph does explicitly foresee the conditions under which the privacy-rights recognised by the first paragraph can be limited by the state. A look at the existing legal exceptions to the protection of privacy and their acceptance by the case-law of the European Court of Human Rights very well shows that the opacity provided by privacy has in fact a rather limited scope. But this does not affect the importance of the fact that the article recognises the principle of a prohibition of interference with an individual's private and family life, home and communications. In certain cases the court ruled categorically against state intervention (for example in respect of homosexual relations).

Art. 8 of the Charter provides a good example of a transparency tool because it organises the channelling, control and restrain of the processing of personal data. Data protection legislation regulates the processing of personal data. It guarantees control, openness, accountability and transparency of the processing of personal data. In principle, thus, data protection law is not prohibitive. As a rule personal data may be processed provided that the data controller meets a number of conditions. The rule is a "yes, but …-rule". Hence data protection is pragmatic of nature: it assumes that private and public actors need to be able to use personal information and that this must be accepted for societal reasons which predominate the concerned privacy interests.

All in all, it can be said that by default privacy is an opacity tool and data protection a transparency tool. This means that data protection also can foresee for opacity rules (*e.g.*, when sensitive data are at hand), while, inversely, privacy can allow for transparency rules, *e.g.*, when telephone taps are allowed under strict conditions (by legal regulation, for certain incriminations, limited in time, with control of police, etc.). This shows again that opacity and transparency tools pre-suppose each other and are intertwined and that devising a good position of the switch is quintessential.

A DANGEROUS BALANCE BETWEEN THE OPACITY OF INDIVIDUALS AND THE TRANSPARENCY OF POWER?

In our former work, Paul De Hert and I [1, 2] have attempted to show that nowadays the focus is way too much on the use of transparency tools. There is too much admitting and enabling regulation, and a lack of prohibitive and shielding regulation. There is too much "yes, but …" and a lack of "no, but …". There is not enough "stop" and too much "go".

In our opinion, the dangers of such an approach are obvious because the conditions linked to transparency rules are never a hurdle to high to take by governments or private actors. "Conditions" have a tendency to turn into formalities, and are very often be emptied of their force. But even more important, without opacity rules or limits protecting individuals, the transparent and procedurally correct dictatorship comes dangerously within reach.

Indeed, an easy example are the far reaching anti-terrorist measures recently taken by various governments (such as the passenger profiling system CAPPSII) or initiatives promoting the interoperability of all kind of personal data processings for police and intelligence purposes. But even more disturbing, is that the same tendency can be detected in the case law of the human rights Court of Strasbourg as the Court tends to overstress the importance of accountability, foreseeability and procedural safeguards relating to privacy limitations, and this to the detriment of the normative and prohibitive drawing of barriers. The Court concentrates too much on the control of the fulfilment of the more formal legality condition for the restrictions of privacy, skipping the check of the necessity of such restrictions in a democratic state. As a result, it can be said that the privacy approach of the Strasbourg Court overlooks the significance of opacity in a democratic state. It is of course understandable that the European judges prefer to focus on much safer issues such as accountability and foreseeability, but aren't our times in need of stronger statements about issues such as the invasiveness of new technological means or the new police powers that are developed within and outside Europe? And are the quasi-constitutional judges in Strasbourg not precisely expect to be the watchdogs of fundamental individual freedoms and rights?

CONCLUSIVE REMARKS

Opacity tools, such as the protection of privacy, imply the making of clear-cut 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 and transparency. 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 interests and principles, liberty threatening and privacy invasive measures could be, exceptionally and regrettably accepted under legally enforced conditions of transparency and accountability. This is, as a matter of fact, the position which Europe has already adopted and enacted in respect of the processing of (non-sensitive) personal data, nowadays regulated by data protection rules.

In general, Paul De Hert and I have argued that today there is an imbalance between opacity and transparency: the emphasis is too much on transparency tools; they have taken too much space. We are convinced of the dangers of such an approach because the procedural and formal prerequisites of transparency tools can easily be met (at large scale) by governments and/or interested third parties. Such an approach might erode what we believe to be the very core of a democratic constitutional state, namely the autonomy of individuals, their self-fulfilment and their participation in public life. It is indeed a very different position to accept that individuals and their actions might be the object of systems of automatic, permanent and real-time monitoring only under stringent conditions, than to categorically refuse it and to ban this possibility. Of course, the latter position can easily be brushed aside as being unrealistic and utopian under the arguments that "technology will not be stopped" and that "any available mean will be effectively used". But the problem with such stance is that it implies we have no power to participate into the further construction of the society we are and will be living in. And that is precisely why dismantling the switch between opacity and transparency in order to replace it by a principle of transparency (power can always be allowed as long as it is accountable) threatens the core of our concept of a democratic constitutional society.

Hence, we should stick to the principle that in an open democratic society there exists a strong and permanent obligation to weigh opacity and transparency tools and to choose which approach is most appropriate in respect of new events and trends. Confronted with new technological developments, parliaments and decision makers will have no other choice than to cope with following questions: how much of what tool is necessary and when? When will opacity (privacy) be called upon, when will transparency (data protection) apply? How to combine the tools appropriately, especially when faced with new challenges, such as today's insistence of various government initiatives on security or the development of new technologies?

Biometrics provide a strong and expressive example both of the necessity to address the issue of opacity and transparency and the complexity of the process. Indeed, the large scale use of biometrics does not only question the position of the individual in society, but it also alters the architecture or nature of this society as such. This implies that one could certainly develop a strong and convincing plea to prohibit the use of biometrics from an ethical perspective, with reference for example to a value as "human dignity", or (and) from a more political perspective claiming such arguments as a "disproportional interference in the individual autonomy" or the "dangers of the control and surveillance society". The mere fact that such concerns are voiced demand a serious consideration of a principled normative and prohibitive policy aiming at protecting the individual's opacity.

It should be added that scientific and technological developments are not inevitable or neutral, which is *mutatis mutandis* also the case for biometrics. Sociology

of sciences has shown that any technological artefact has gone through many small and major decisions that have moulded it and given it its actual form. Hence, the development of information technology is the result of micro politics in action. Technologies are thus closely linked to social organization, cultural values, institutions, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road toward a serious political, democratic, collective and legal assessment of technology. This means that technologies cannot be considered as *faits accomplis* or extra-political matters of facts. On the contrary they are matters of concern or "issues" and require a political state of affairs to be made [4, 5]. In this process the difficult calibration and the handling of the switch between policies of opacity and policies of transparency cannot but be at stake.

The process of opting for opacity or for transparency is actually still more complex than already suggested, because the concrete questions and their contexts do justly influence the position one must construct. Indeed, the question of the use of biometrics for border controls is different than the question of its use for national ID-cards, in criminal investigations, in fighting terrorism or pandemics, for access control at soccer games and in dancings, or say, for the selling of hamburgers. Rules at a general level just won't do. Which makes the issues at stake still more difficult: a balance between opacity and transparency must be searched in respect of each particular or generic set of problems.

Submitted on invitation.
Accepted on 4 October 2006.

References

1. De Hert P, Gutwirth S. Making sense of privacy and data protection: A prospective overview in the light of the future of identity, location-based services and virtual residence. In: *Security and privacy for the citizen in the post-September 11 digital age: A prospective overview*. IPTS-EC-JRC, European Communities; 2003. (Technical Report Series, EUR 20823 EN). p. 111-62. Available from: ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf.
2. De Hert P, Gutwirth S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In: Claes E, Duff A, Gutwirth S (Ed.) *Privacy and the criminal law*. Antwerp/Oxford: Intersentia; 2006. p. 72-6.
3. Tadros V. Power and the value of privacy. In: Claes E, Duff A, Gutwirth S (Ed.) *Privacy and the criminal law*. Antwerp/Oxford: Intersentia; 2006. p.106-09.
4. Latour B. From Realpolitik to Dingpolitik. How to make things public? In: *Making things public. Atmospheres of democracy*. Latour B, Weibel P (Ed.) Karlsruhe/Cambridge Massachussetts, ZKM-Zentrum für Kunst und Medientechnologie: The MIT Press; 2005. p. 14-41.
5. Latour B. Why has critique run out of steam? From matters of fact to matters of concern. *Critical Inquiry* 2004;30:225-48.