

Identity control, activity control: from trust to suspicion

Meryem MARZOUKI*

Abstract

Processes introducing biometric identity control and communicating activity controls through data retention sign, in France and Europe, a reversal of perspective. Taking into account the legislative and regulatory transformations as well as the strategies of government and industry actors, and considering the various means of consent from the general public, we will analyze several levels of this change of paradigm: security objectives centered on intelligence rather than legal investigation; legislative and judicial proceedings oriented towards soft and contract law; intervention of private actors with prerogatives of public power; preventive rather than repressive civil or penal actions, specially through the use of technical means; sometimes inversion of the burden of the proof, requiring proving innocence rather than guilt. This results in the change from a conception of society based on mutual trust into a situation of generalized suspicion.

Key words: Biometrics, Retention, Security, Information technology, Political aspect, Legal aspect, France, Private life protection, Political sociology.

CONTRÔLE DES IDENTITÉS, CONTRÔLE DES ACTIVITÉS : DE LA CONFIANCE À LA SUSPICION

Résumé

Les processus d'introduction des contrôles biométriques d'identités et des contrôles d'activités communicationnelles par la rétention de données signent, en France et en Europe, un renversement de perspective. Prenant appui sur les transformations législatives et réglementaires et sur les stratégies des acteurs publics et industriels, tout en étudiant les différents ressorts du consentement de la population, nous analyserons plusieurs niveaux de ce changement de paradigme : objectifs sécuritaires axés sur le renseignement plutôt que sur l'investigation judiciaire ; procédures législatives et judiciaires orientées vers une contractualisation du droit ; interventions d'acteurs privés dotés de prerogatives de puissance publique ; action civile ou pénale préventive plutôt que répressive, notamment à l'aide de dispositifs techniques ; charge de la preuve parfois inversée, nécessitant la preuve de l'innocence plutôt que de la culpabilité. Il en résulte qu'une conception de la société fondée sur la confiance mutuelle se transforme en une situation de suspicion généralisée.

Mots clés : Biométrie, Rétention, Sécurité, Technologie de l'information, Aspect politique, Aspect juridique, France, Protection vie privée, Sociologie politique.

* Laboratoire d'informatique de Paris 6 (LIP6/PolyTIC-CNRS) –104, avenue du Président Kennedy, 75016 Paris, France ; Meryem.Marzouki@lip6.fr

Contents

- | | |
|---|--|
| I. Introduction | IV. <i>Beyond the privacy issue: the breach in the social contract</i> |
| II. <i>A national example : the French scene</i> | References (23 ref.) |
| III. <i>Main trends in ICT-based public security policies</i> | |

I. INTRODUCTION

On January 11, 2004, only some days after the launching by the United States government of its *US-VISIT* program¹, the Italian philosopher Giorgio Agamben published an opinion in the French daily newspaper *Le Monde*², announcing that he canceled his visiting course at New York University, scheduled later in the same year. Saying “No to the bio-political tatoo”, Agamben referred to the bio-political power – a concept he theorized after Michel Foucault – to explain the reasons of such a decision.

As defined by the US Department of Homeland Security, the *US-VISIT* program “*requires that most foreign visitors traveling to the U.S. on a visa have their two index fingers scanned and a digital photograph taken to verify their identity at the port of entry*”. According to Agamben, this use of biometrics for routine border control crosses “*the thresholds in the control and the manipulation of human bodies*” defining the limits of a new bio-political era.

The *US-VISIT* program is only one element of the whole integrated control and surveillance system elaborated in the USA [1] for years, though with a special acceleration after September 11 attacks, which is not only targeted at foreign visitors, but also at US citizens and residents. Similar control architectures are being developed and consolidated at the international level [2], including in Europe, notwithstanding a more comprehensive legal edifice protecting the right to privacy, to the extent that prominent US privacy lawyers take it as the example to be followed by the United States [3].

From simple logistic means of implementation, ICTs have become integral part of public security policies in Europe as well. They are now used for the control of people’s movement, of the circulation of any kind of information resulting from the dematerialization of procedures, as well as the control of communications. They thus lead to the setting up of large databases and to the interconnection of information, allowing, to an unprecedented extent, to reveal the intimacy of persons, to map their activities, and to identify networks interconnecting them.

How public security policies in Europe have developed in such a way? Is this situation a consequence of September 11 attacks in the United States or has simply this event accelerated and amplified a previous movement? How may the process of mutual consolidation and reinforcement of national and European policies be analyzed? How can they be replaced in the international process? What are the *non dits* (hidden facts) of these policies, do they have

1. U.S. Department of Homeland Security press release, January 5, 2004.

2. Giorgio Agamben, *Le Monde* dated January 11, 2004 (« Non au tatouage biopolitique »).

other purposes than those mainly put forward? To what kind of debates have they given rise - or not - in the society? Would these trends be pursued in the following years or are social resistances emerging? More globally, should the observed transformations in the application of the rule of law be analyzed as a consequence of the use of ICTs in the implementation of security policies, or as the outcome of a coherent process constituting the very objective of these policies?

This paper wishes to explore these questions, starting from empirical research works allowing to precisely inventory the situation in France and at the European level. The French national example will specially be presented to support the analysis.

II. A NATIONAL EXAMPLE: THE FRENCH SCENE

For the sake of clarity in setting the scene, we will only briefly – and certainly non exhaustively – present in this section the main legislative and regulatory instruments adopted in France. Developments at the world level are yearly documented in the annual report on *Privacy and Human Rights*, published by the Electronic Privacy Information Center since 1999 [2]. Particularly since year 2001, after September 11 attacks, quite similar developments may be observed in different countries, especially in the European Union (EU), considering the legal harmonization efforts in this regional political entity, especially in criminal matters [4]. At the larger level of the European continent, the Council of Europe (CoE) Convention on cybercrime³ imposes to CoE member States, and additional countries that ratify this international Convention, a certain level of criminal law harmonization in view of a more developed cooperation between national law enforcement authorities [5]. On a more case by case basis, some unilateral initiatives like the US-VISIT program spread out to other countries in the world, either as a reciprocity measure claim or simply because the US government fortunately opened the way [6]. Finally, police and identification issues and projects in different countries, particularly using biometrics, have recently been reviewed in [7].

Long before the adoption of the EU Data Protection (DP) Directive⁴ in 1995, France has enacted its own DP Act⁵ as early as in 1978, after a public scandal following the announcement of a government project, called SAFARI, of interconnecting all files detained by the public administration on individuals⁶. This DP Act has also created the French DP Authority, the CNIL, as the first French independent administrative authority, with the mission to protect public liberties [8]. The Act was revised in 2004⁷. Although initially only undertaken to comply with the need to transpose into national law the EU DP Directive, this revision, which process started in July 2000, received strong criticisms by French human rights and civil liberties organizations as well as by former CNIL commissioners⁸. Critics of the new text clai-

3. CETS N°185. Adopted in Budapest on November 23, 2001, entered into force on July 1, 2004.

4. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

5. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

6. The SAFARI project was unveiled by an article in *Le Monde* dated March 21, 1974 and entitled "*SAFARI ou la chasse aux Français*" ("SAFARI or French people hunting").

7. Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

8. See, inter alia, two opinions respectively published by representatives of the two groups in *Le Monde*: "*Big Brother se rapproche*" (April 14, 2004) and "*Il faut sauver la loi informatique et libertés*" (July 14, 2004).

med that it was a severe step backwards in terms of privacy protection and the respect of the rule of law. However, besides these interventions in the public debate, and despite the action from the Parliamentary opposition against the new text, not only the revision was adopted and, except for a single provision, found constitutional [9], but also, interestingly enough, this didn't result in much public scandal in the opinion, contrarily to the situation that occurred almost 30 years before.

Actually, this situation does not sign a sudden change in the French opinion, but is rather a result of its progressive though confirmed disinterest from privacy issues. A tentative analysis of this process is provided in the sequel of this paper, however one should note at this step that this evolution may also be due to the number of important legislative and regulatory measures that have been adopted in France in the mean time.

II.1. Mapping activities, communications and movements

Like many other countries, France has seen an intense legislative and regulatory activity after September 11 attacks.

In November 2001, only two months after this event, the Daily Safety Law (*Loi sur la sécurité quotidienne*⁹ or LSQ) was adopted. This law now rules, inter alia, the retention of electronic communication data regime, through its so-called anti-terrorism provisions added in emergency at the latest steps of the LSQ adoption process. Although explicitly claimed to be a response to the new international situation, these provisions were extracted from a draft law on the Information Society, introduced on June 13, 2001 and prepared since 1999. With the LSQ, French Internet Service Providers (ISPs) were required to store log files on all their customers' activities for up to one year, and the government was granted access to private encryption keys.

In March 2003, the Internal Safety Law (*Loi sur la sécurité intérieure*¹⁰ or LSI) was enacted. Some of its provisions deal with electronic communications. They authorize the immediate access by law enforcement authorities to the computer data of telecommunications operators, including Internet access providers, as well as of almost any public or private institute, organization or company. The second important measure authorizes the search without warrant of any information system, provided that the data is accessible through a network to which the computer being searched with a warrant is connected. Finally, the LSI has perpetuated the so-called anti-terrorism provisions of the LSQ, which were initially valid only until December 2003.

The trend has also been pursued after the revision of the French DP Act, with the adoption in January 2006 of the Anti-Terror Act (*Loi relative à la lutte contre le terrorisme*¹¹). This law grants increased powers to the police and intelligence services, thus undermining the protection of formal judicial procedures. It also extends telecom data retention possibilities, by assimilating cybercafe owners and WiFi providers (whether for free or with payment) such as bars, restaurants and hotels to telecom operators. Any logged data may also be seized directly by the police, without any judicial order, "in order to prevent acts of terrorism".

9. Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

10. Loi n° 2003-239 du 18 mars 2003, Loi pour la sécurité intérieure.

11. Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

The Anti-Terror Law also allows for the control and mapping of people's activities and movements. It extends the use of video-surveillance¹², authorizing private parties to install CCTV cameras in public places "likely to be exposed to terrorist acts" and in places open to the public when they are "particularly exposed to risks of aggression or theft". In case of emergency, CCTV cameras may be installed prior to any authorization. Furthermore, in its article 8, the Law allows the police to automatically monitor cars on French roads and highways, taking pictures of license plates and people in the cars, with various purposes ranging from the fight against terrorism to the identification of stolen cars. The same article provides for the monitoring of street gathering during "big events". Finally, the law provides, in its article 7, that the Ministry of Interior may process PNR (passenger name records) data collected on any travel by air, sea or rail to or from non-EU countries. This article has the claimed objective "to improve border controls and to fight against illegal immigration". France has been then the first EU country to follow the example of the US unilateral decision imposing the transfer of EU citizens' PNR data to US customs and border control authorities¹³.

Soon after the adoption of this Anti-Terror Act, in March 2006, the long-awaited application decree regarding LSQ data retention provisions was published – almost 5 years after their introduction in so-called emergency. This decree¹⁴ also provides for application measures of some articles of the Anti-Terror Act. It determines the duration of data retention by telecom operators, setting it to the maximum time allowed by the LSQ (one year) and the type of data to be retained (all kind of data involved in a telephone or Internet communication, except its content).

The interested reader may find further descriptive details on these developments in our contribution to [10] (chapter on *French Republic*) and in comprehensive dossiers, on most of legislative developments and actions and campaigns organized in protest by human rights and civil liberty organizations, made available by the French digital rights NGO IRIS¹⁵.

II.2. Increasing the use of biometrics

Among the many indexing files existing in France and created for the purpose of public security and the preservation of the public order, biometric files are increasing both in number and in quantity of indexed information. A list of these current biometric files with their characteristics may be found in [11], however, one of them needs to be presented here to allow better comprehension of the sequel of this paper. The National Computerized File of Genetic Data (*Fichier national automatisé des empreintes génétiques* or FNAEG), created in 1998 by law¹⁶, contains the DNA traces found on a crime or offense scene, as well as the DNA profiles of persons either convicted or only suspected of a crime or an offense. These data are kept 40 years for convicted persons and 25 years for suspected persons. Access to these data is granted to law enforcement authorities.

12. Ruled until then by a 1995 Law, Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

13. On the US-EU PNR issue, see [6].

14. Décret n°2006-358 du 24 mars 2006, relatif à la conservation des données des communications électroniques.

15. IRIS dossiers available on LSQ, Information Society draft Law, I.S.I, French and European data retention issues, and US-EU PNR deal, all at <<http://www.iris.sgdg.org/actions>>

16. Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

The use of biometric identifiers is also increasing for immigration and border control. France is taking its part in the EU trend to extend their use in visas, and other travel and immigration documents. On November 2003, the Immigration Law¹⁷ has generalized the use of biometric techniques for visa delivery and border controls, and the storing of all visa requesters' fingerprints and biometric pictures in databases for further processing. In application of this law and its application decree¹⁸, an experimental file has been created in November 2004 for two years, as a complement of the French worldwide visa requests management system called RMV2 (*Réseau Mondial Visas 2*) linking the central administration to French Consulates abroad and communicating with the Schengen Information System (SIS) [12]. This additional file contains the digitized photograph and all fingerprints of persons asking for visas at some French consulates chosen for the experiment. These data are conserved two years for a short-stay visa request, five years for a long-stay visa one or in case of visa denial. Access to this file is allowed to some border police officers at some French airports, harbors or land frontiers [11]. Biometric identifiers may be included in an electronic chip on the visa. This process is undertaken by France, following the request of the European Commission before a generalization of the experiment. In 2006, a new decree¹⁹ has further extended the purposes of the file so as to allow identity controls by the police everywhere in France, and not anymore only upon entry at the borders. The same decree has also extended the collection of biometric identifiers to other EU member State consulates, and the access of these data to other police officers than border control ones. Finally, it has extended the experimentation by one additional year, delaying its assessment to November 2007.

II.3. INES, the French biometric ID card project

Centralized files and databases for biometric identification then already exist, and are more and more shared with other governments²⁰. However, they are not anymore restricted to identify categories of people felt dangerous for the society (criminals and undesirable foreigners), to be now extended to the “honest citizen”, whose identity was, until recently, only controlled to check his absence from the central file [14]. The “big one” is thus coming, with the advent of the biometric passport and the biometric ID card projects flourishing in numerous countries. The international situation and issues around the biometric passport and biometric ID projects are well documented in a *London School of Economics* report²¹ [15], we will thus restrict ourselves to a quick presentation of the French biometric ID card project of “Secured Electronic National Identity” (*Identité nationale électronique sécurisée* or INES).

17. Loi n° 2003-1119 du 26 novembre 2003. relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité

18. Décret 2004-1266 du 25 novembre 2004.

19. Décret 2006-470 du 25 avril 2006.

20. In Europe, a new step in the cross-border cooperation has been achieved in May 2005 with the Prüm Treaty [13], signed by 7 EU member States, including France, “in view to combat terrorism, cross-border crime, and illegal immigration”. This Treaty allows for the exchange of DNA profiles, fingerprints and other personal and non personal data. Most of the provisions of this Treaty are currently in the process of being incorporated into the EU legislation (see http://www.polytic.lip6.fr/article.php3?id_article=166).

21. See also, for latest developments, the dedicated information from Privacy International, available on the NGO website at <<http://www.privacyinternational.org>>

The INES project has been introduced through the launching of a public debate organized by the “Internet Right Forum” (*Forum des droits sur l’Internet* or FDI), a private association mainly funded by the French government. The then French Minister of Interior commissioned the FDI to organize this debate, recognizing that “legitimate questionings may arise in the public opinion on such a project” and mandating the FDI to “inform the opinion on this dossier and collect citizen’ opinions and proposals”, as written in his mission letter²². The first (and only, as of March 2007) public presentation document of the project, dated March 1st, 2005, has been released at this occasion. According to this document and to an interview of the then Minister of Interior²³, the project aimed at providing the whole population by 2007 with a new ID card, with a contact-less chip containing the civil status of the citizen as well as two biometric identifiers: photograph and fingerprints. These data would be filed in centralized databases. The card would be mandatory and would also include the address of the holder. It would also be programmable, to become an electronic *portfolio* that could be used for e-administration as well as commercial electronic transactions.

This INES project received very strong criticisms in France, well relayed in mainstream medias. The debate organized online and offline by the FDI led to a critical report calling for a number of actions and modifications before implementing the project. The CNIL, who had not been asked for any opinion by the government, decided to organize a number of hearings²⁴ on the project, which were also very critical. The Commissioner in charge of the dossier publicly expressed many times that “the CNIL has always had reservations on the constitution of central biometric databases”. Last but not least, a large protest campaign has been organized by human rights and civil liberties organizations together with unions of lawyers and magistrates, all grouped in a “coalition against the INES project” to demand the withdrawal of the project. At a press conference held to launch the coalition, they declared: “The government recognizes that the ultimate goal of the project is to set up a universal card which integrates the identity, the benefit of social rights and the ability to make private transactions; the idea is to make the individual totally transparent to both public authorities and commercial actors”²⁵.

However, controversies around the introduction of an ID card *per se* are left out of the French debate, contrarily to other countries. In these latter cases, the situation leads to some difficulty in understanding what is exactly at stake: introducing an ID card in a country whose culture and history is not used to such a card, or the features (universal, centralized, biometric...) of this ID card. Such a mix of issues may prevent objective discussions, especially between communitarian and libertarian positions in Anglo-Saxon countries [16, 17].

The harsh critics against the INES project have led the (new) Minister of Interior publicly declare on June 2005 that the project “will profoundly impact the daily life of French citizens for a long time. If European provisions impose us to quickly set up a biometric passport, the situation is different for the electronic ID card. I don't want us to engage in this project without having taken the necessary time to think about all its consequences.”²⁶ As of March 2007, a new public version of the INES project is still awaited. The future of this project is

22. The website of this public debate, with archives of all relevant documents, is available at <http://www.forum-internet.org/carte_identite>

23. Dominique de Villepin was interviewed by France-Soir on April 11th 2005.

24. Information available at <<http://www.cnil.fr/index.php?id=1817>>

25. The website of this coalition, with all relevant documents, is at <<http://www.ines.sgdg.org>>

26. Nicolas Sarkozy, French Minister of Interior, public declaration on June 20, 2005, at the meeting of French prefects

now subject to the results of the French presidential and legislative elections, scheduled in May and June 2007, respectively.

III. MAIN TRENDS IN ICT-BASED PUBLIC SECURITY POLICIES

This quick panorama of the French scene, in line with legal and regulatory developments elsewhere in the world and more particularly in Europe²⁷, leads to the identification of some main trends in public security policies relying on ICTs and/or in the information and communication field.

Three main characteristics of this movement appear as the signs of profound transformations. The State more and more gives up some of its prerogatives, delegating parts of its sovereign powers to private actors. At the same time, the State consolidates its own logic of police control, circumventing judicial, administrative, and citizen safeguards. And this is happening in a growing climate of social consent to – when not demand for – these transformations.

In practice, in depth analysis of the political discourse and detailed examination of the legal and regulatory evolution highlight the practices at play. Policy laundering is intensively used as a mean to introduce new regulations at national level. Once a control instrument has been introduced and accepted in a given context, its purposes and operational conditions are systematically later extended to fulfill new objectives. Hidden agendas become then revealed: from the fight against terrorism, the purposes soon transform into the fight against illegal immigration, the restriction of legal immigration, and the fight against minor criminality. Taking into account that these security policies make use of ICT hardware and software equipments, the observed intense lobbying of economic actors in the field seems fruitful.

In the mean time, a “culture of security” is emerging and consolidating in the society, with a serious erosion of the sense of privacy.

As a result, within only some years or decades, in depth substantive transformations of the rule of law principle, often only through procedural regulation, have occurred, possibly even leading to breaches in the social contract.

The sequel of this paper will develop this thesis, analyzing the arguments put forward and illustrating them with concrete examples.

III.1. Delegating State powers to private actors

Delegating State powers to private parties is by no mean specific to security issues and not even to the regulation of technological networks. As analyzed in other sectors of public policy making, this is one of the characteristics of a shift from *government* to “*governance*”. However, the combination of the technical complexity involved by electronic networks with

27. For international developments, see annual *EPIC* reports since 1999 [2], as well as the weekly newsletter about legal and regulatory aspects of the information society, *quicklinks*, edited by Richard Swetenham (<<http://www.qlinks.net>>). For more in-depth and day to day European developments, refer to the biweekly newsletter of the European Federation *EDRI*, *edri-gram*, (<<http://www.edri.org/edrigram>>)

the claimed “need for efficiency” in the discourses on security makes this general trend particularly tangible here.

In the field of Internet communications, Internet Service Providers (ISPs) play a pivotal role as the unavoidable technical intermediary. Ian Kerr and Daphne Gilbert note that, “in the context of investigatory information, the architecture of the Internet [...] requires an ISP to intermediate between two potentially conflicting roles: (1) its role as the trusted steward of its clients’ personal information and private communications; (2) its role as a party in possession of information that might assist in law enforcement.” Elaborating on this specific role of ISPs, they show how they may act as “agents of the State”, and they analyze in particular the procedural provisions of the CoE Convention on cybercrime which assign them to the collection of investigatory information [18].

In [19], we discuss other uses of procedural measures to extend the prerogatives of ISPs and other private parties. Such procedural measures include: the limitation of ISPs liability for unlawful content they may be hosting, while authored by one of their subscribers, provided that some conditions are respected; the use of contractual regulations either through ISPs code of conducts or specific subscription clauses; the increasing promotion of alternative dispute resolution mechanisms, especially when implemented in on-line form.

New legislative and regulatory developments on the French scene presented in this paper provide additional examples. In the revised French DP Act, two provisions are illustrative: article 9 allows intellectual property rights societies to create private records of rights infringers; article 8-II lists additional exceptions to the principle forbidding sensitive data collection, by authorizing the “data processing in view of [...] exercising judicial rights”. As highlighted by the Parliamentary opposition in its constitutional challenge to this law, this new provision may be applicable to any private company. Another example is provided by the new Anti-Terror Act, when it extends data retention obligations to cybercafes and wireless Internet access providers, compelling hotels, cafes, restaurants managers, if this law is to be effectively applied, to control the identity of their customers.

III.2. Circumventing democratic safeguards

The circumvention of democratic safeguards against arbitrary power decisions, such as judicial, independent administrative, and citizen controls, is also becoming common practice. Two main arguments are used to justify these practices: the length and the cost of the judicial process, and the need for preventing infractions. Many recent laws in France have then allowed the intervention of the police without any judicial order, the most recent one being the Anti-Terror Act.

A particular case illustrating this trend in France is the circumvention of the DP Authority intervention. As already explained in this paper, the CNIL was created in 1978 with the mission to protect public liberties. One of the important mean it was given to this end was the need for the government to take administrative measures (such as decrees) only when, after consultation, the CNIL and the *Conseil d’État* (the French highest administrative court acting as the government advisor) end with the same opinion (“*avis conforme*”). In practice, this process was granting the CNIL a kind of “veto right” on some government decisions. Indeed, through the negotiating process between the CNIL and the *Conseil d’État* to reach a common

opinion, the initial decision would need to be downsized in order to comply with the two cardinal principles of proportionality and limited purpose in privacy and personal data protection matters. This safeguard against arbitrary decisions infringing privacy has disappeared with the revision of the DP Act. Articles 26 and 27 of the new Act have suppressed the need for this *avis conforme*, and CNIL's opinion has become consultative only for regulatory processes like decrees and ministerial orders, including when the collection and processing of sensitive and biometric data are concerned. This safeguard circumvention has already been used three times since the enactment of the new law, in November 2004, August 2005 and July 2006²⁸. First two cases relates to visa issuing to foreign visitors for short or long stays in France, and the third case to the creation of a new file indexing foreign visitors who stayed illegally in the country (also filing data of their children, their hosts and their visitors in retention centers). In first two cases, the CNIL expressed serious reservations, which were not considered by the government. In the third one, it missed the two-months legal delay to give its consultative opinion...

More cases of CNIL safeguard circumvention are likely to arise, since more and more French laws are referring to further administrative decrees for their application. This is actually the case of the new Anti-Terror Act.

III.3. Policy laundering

One may wonder at this step how it comes that processes such as those described here may be conducted in an almost generalized climate of social consent, 30 years after the public scandal which led to the DP Act. The explanation is likely to be found in a growing "culture of security" in the public opinion. It is thus worth exploring how social consent has progressively been manufactured – or has it manufactured itself? – using a political discourse legitimating legal and regulatory developments which are actually violating fundamental rights and freedoms as well as basic democratic principles.

A more and more common mean of introducing such measures is to justify them by external obligations: "*We must comply with international regulations!*" and (in EU member States) "*It's a Brussels requirement!*" are so frequently heard arguments everywhere in the world that three civil liberties organizations have set up a dedicated project to fight what they call "policy laundering". As they define it: "*Just as money laundering describes the cycling of illegitimate funds through outside institutions in order to enter them into legitimate circulation, so does policy laundering involve the cycling of policies that lack political legitimacy through outside intuitions in order to enter them into circulation despite their lack of acceptance*"²⁹.

Such kind of policy laundering is also at play in France, and the introduction of the INES project is a particularly illustrating example. The French government claimed that this project was necessary because of international standards defined by the International Civil Aviation Organization (ICAO) and by the EU regulations, as well as by the American government unila-

28. Details on these cases are available through the NGOs that challenged the administrative decisions, see <<http://www.iris.sgdg.org/actions/fichiers>>

29. See the website of this project at <<http://www.policylaundering.org>>

teral request for biometric passports to visit USA. However, opponents to the INES project argued that first ICAO standards, EU regulation and US request only concern passport and other travel documents (and not national ID cards) and second that, as regards ICAO and US government, only one biometric identifier was required, the digitized photograph (and not fingerprints). Moreover, and this is a typical policy laundering effect, it is obvious that the French government takes an active part in international and regional regulations, even when discussions take place behind closed doors and without any democratic control, like in the case of ICAO and the EU council meetings, as civil liberties organizations constantly denounces. In addition, France participates for many years to discussions in the G8 framework on the use of biometrics, as the press reports.

III.4. Extending control conditions and purposes and fulfilling hidden agendas

As already recalled, there are two cardinal principles in the national and EU legislation in privacy and data protection matters: proportionality and limited purpose. This means that any measure taken in this field should be strictly proportional to its objectives, and that these purposes must be legitimate and precisely defined.

However, in many cases, measures taken have been further extended in terms of purposes and operational conditions. This particularly happens when the control instrument has been set up under emotional circumstances facilitating its acceptance, and is then extended to long-term structuring decisions when people got used to it. The FNAEG file is one of these examples. It was originally created in 1998, its use being restricted to serious sexual offenses like rape and child abuse. The FNAEG purposes have then been further extended by three successive laws in 2001, 2003 and 2004, as well as by three decrees respectively adopted in 2000, 2002 and 2004 [11]. Currently, the FNAEG concerns the persons condemned or simply suspected of almost any prejudice against property or person. The result is that this file is currently being used to mandatory indexing DNA profiles of trade-unionists or activists fighting GMO dissemination in the country³⁰.

Extension is also realized over time, like it happened with the US Patriot Act sunsets. A French example is the so-called “time-limited” provisions of the LSQ, which were never assessed, since another law, the LSI, made them perennial before the time limit initially set to December 2003. Socialist Senator Michel Dreyfus-Schmitt, from the political majority when the LSQ was adopted, declared at that time: “we may hope to be back to the legality of the Republic, to call a spade a spade, after December 31, 2003 or even before this deadline” [19]. He was wrong, though perfectly illustrating our point.

This process of extending surveillance and control conditions and purposes may be a way to fulfill hidden agendas. While the fight against terrorism is obviously a legitimate and necessary objective in itself, it may also constitute the perfect alibi to social control measures.

This appears with the mix of purposes of a given decision. For instance, provisions intended to fight terrorism are sometimes used to fight minor crimes and to control street demonstrations and public gatherings, which obviously infringes the proportionality principle. This

30. See report on such cases in the press at <<http://www.humanite.fr/journal/2006-08-26/2006-08-26-835494>>

is the case with the new Anti-Terror Act and its provisions allowing to take photographs on highways and during big public events. Furthermore, the PNR provisions of this Act clearly target non EU immigrants and even foreign residents, especially those from North Africa, since they regularly travel by sea to spend holidays home, while recent terrorist bombing in Europe were perpetrated by nationals. These provisions have rather other purposes, that is, to fight illegal immigration and to restrict legal immigration.

Hidden agendas also show through political legitimating discourses for new surveillance and control measures. The justification for the INES project insisted on massive frauds in identity documents for criminal purposes and in the fiscal, social and medical sectors to obtain undue benefits. The INES project was then presented to the honest consumer and taxpayer as the panacea to fight these parasitic social behaviors. However, despite the many public requests from the project opponents, no statistics on these frauds was ever provided.

III.5. An economic and managerial logic at play

Beyond the security objectives, an economic and managerial logic is also at play with the introduction of biometrics in public security policies. First of all, biometrics is a huge market, currently only in emergence and with high promises. According to the International Biometric Group, a biometric industry's consulting firm, "global biometric revenues are projected to grow from \$2.1B in 2006 to \$5.7B in 2010, driven by large-scale government programs and dynamic private-sector initiatives"³¹.

Major choices made by governments have obvious structuring effects on this market, especially when they decide to choose some biometric techniques over others, given that different national industries are leading different markets segments. There have been intense discussions at G8 meetings in 2003 in order to decide which kind of biometric identifiers (digitized photograph, fingerprint, iris) to use in passports and other travel documents. Attending this meeting as French Minister of Interior, Nicolas Sarkozy declared: "the French tradition is fingerprint"³². Not only is it a tradition, but also the leading advantage of the French biometric industry, with the French group *Sagem Défense Sécurité* being the world market leader. This governmental will to support the national industry has been confirmed in December 2005, when the Secretary general of the French Interior Ministry was asked whether a new version of the INES project would be soon released. "We are in a situation where, through our decisions, we may hamper or not the French industry know-how, which is, in this field [biometrics], considerable", he declared³³.

Besides this economic logic in support of the biometric industry, indirect benefits are also expected in various other economic sectors from the rationalization of processes and procedures the use of biometric identification allows, like fast flows at supermarket cashiers... or at border control [20]. This managerial logic is expected to develop in the future.

31. See IBG press release dated January 23, 2006, at <http://www.biometricgroup.com/press_releases/pr_2006_BMIR_2010.html>

32. See a ZDN et report dated May 7, 2003, available at <<http://www.zdnet.fr/actualites/informatique/0,39040745,2134363,00.htm>>

33. Le Monde, December 29, 2005.

III.6. The erosion of the sense of privacy in the society

All these trends in ICT-based public security policies are developing in a growing social consent climate. In France, for instance, the opposition to the INES project till now shouldn't be misleading. When the FDI released its report on the public debate commissioned by the French Ministry of Interior, it also published the result of a poll on the INES project. While the report was very critical, reflecting the opinions of participants to the online and offline debates who were experts, NGOs and concerned citizens voluntarily taking part in the debates, the poll was conducted on a representative sample of the French population, and expressed quite different feelings: 74% were in favor of the project, with only 25% against it. Notwithstanding usual reservations on these kinds of poll, such a result calls for cautious provisions on the opposition to the INES project.

When searching explanations to this social consent, one needs to go beyond the manipulation of the "insecurity feeling" and the legitimate fears provoked by September 11 events and subsequent attacks in Europe and elsewhere. They are certainly not the only origins of such a massive consent in the society. The technological society has been theorized, analyzed and criticized for almost a half century. However, never before such an erosion of the sense of privacy in the society was reached. This phenomenon may probably be explained by the conjunction of four factors: the use of techniques has become commonplace; maximal convenience and comfort is looked for; the human body and most intimate information have become tradable; new control techniques have become less tangible.

People are getting more and more used with technical devices, and there is a growing appropriation of ICTs by the general public in all human activities: public and private, professional and personal. In this context, the technical device appears more as a necessary tool than a mean of controlling individual's activities. It has been so well domesticated that it cannot anymore represent any danger. Once well mastered, it may be used as a mean of control by the individual of the access to his private space, his information and his goods, or even to himself (by managing his availability to others), according to his own choices. It is finally a mean of domestic control and surveillance. In summary, not only an appropriation of the technique is occurring, but also an appropriation of the technical control.

The convenience argument is often used as a complement to the numerous advantages of digital and biometric techniques. Gain in time, burdenless procedures, minimized queuing, paperless identification... are only some of the nice features of their daily use, as reported by interviewed users, although interviews show contradictory feelings [20]. "One-stop shop" and "shopping right after jogging"³⁴ may be the slogans of digital and biometric techniques introduction in e-administration and commercial activities, respectively.

In line with social changes and at the meeting point between technical devices and market mechanisms, a third phenomenon appears, which leads to the trading of individual's privacy and most personal data, that have become the main value of e-commerce. New marketing techniques do not target generic categories of consumers anymore, they rather use individual profiles. And the individual consumer has himself developed subverting strategies to benefit in his turn from the commercial value of his personal data by e.g. using "free" services or experiencing the "V.I.P. effect" of belonging to a distinguished club of customers. From a civil right, privacy then becomes assimilated to a property right [21].

34. We refer here to supermarkets experimenting payment by fingerprint at the cashier, promoted by the biometrics industry as making shopping a "hands-in-the-pocket" activity.

Finally, resisting control is as much difficult as its perception decrease, especially when it becomes commonplace and painless. This is exactly what happens when control is made through technical devices. First, the technical device intermediates between the controlled individual and the human controller – especially the policeman – whose action, consisting in the collection of data, is executed at a distance. This is specially the case when CCTV and biometrics techniques are used. Second, the control technique used may avoid the perception of the control and of the data collection. This happens with the use of RFID chips, and of biometric data which can be collected as traces left by people in their everyday activities, even without their knowledge. This applies to fingerprints, but also to facial recognition since photographs may be taken in public spaces.

IV. BEYOND THE PRIVACY ISSUE: THE BREACH IN THE SOCIAL CONTRACT

This increasing move towards a distant control with consent is an integral part of the transformation over time from direct and constrained surveillance into indirect and pacified control [14].

However, additional changes are occurring. This paper has shown how any new public security measure, or extension of an already existing one, is motivated, in the discourse of its proponents, by a necessary fight against terrorism, and by an equally necessary “balance” to find between “freedom and security”. However, the systematic, generalized and global character of the use of control and surveillance technologies hardly leaves any control in the determination of a balance point, provided that such a balance may be considered between established and State binding rights and freedoms, and a security objective relying on fuzzy and unstable concepts.

In addition, the structuring character of the implementation of such measures does not leave much margin of maneuver to tentatively get “back to the normal situation”, once gone the threat they claim to face. “Exceptional measures”, duly introduced as such and legally accompanied by “sunset provisions” in order to periodically re-examine their relevance, lead to irreversibly implemented technical standards, to long term structuring of an economic sector, to durably established social behaviors, as well as, more globally, to question fundamental aspects of the rule of law.

With the instauration of this massive control of individuals, have we indeed reached the “generalization of the state of exception”? According to Agamben, “the state of exception is not a dictatorship [...], but a space devoid of law, an anomie zone where all the legal determinations – and first and foremost the very distinction between what is public and what is private – are deactivated” [22].

Privacy is probably not anymore the adequate scheme to analyze new developments in public security and identification policies. Current developments have taken us beyond the issue of privacy and personal data protection. The very foundations of the social contract between the citizen and the State are being seriously eroded. Legal and regulatory trends in France, Europe and at the international level have already shifted from targeted surveillance of a given person under legal investigation to a systematic and generalized control of everyone, for preventive intelligence purposes, signing a reversal of perspective: suspicion has

become the rule and not anymore the exception [23]. With the introduction of biometric identification, the perception of identity is moving from declarative and based on mutual trust to reified and intangible. In the end, power relationships between the citizen and the State are deeply transformed, breaching a social contract once founded on the presumption of mutual trust and on the preservation of everyone's freedoms.

Manuscrit reçu le 18 octobre 2006

Accepté le 11 juillet 2007

REFERENCES

- [1] CEYHAN (A.), La biométrie: une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaines. *Les cahiers de la sécurité* (1st quarter 2005), n° 56, pp. 61-89.
- [2] EPIC, PI, Privacy and Human Rights. An international survey of privacy laws and developments. *EPIC*, Washington (1999).
- [3] SOLOVE (D. J.), ROTENBERG (M.), Information Privacy Law. *Aspen*, New York (2003).
- [4] MONTAIN-DOMENACH (J.), Le droit de l'espace judiciaire pénal européen : un nouveau modèle juridique ? *Cultures & Conflits* (Summer 2006), n° 62, pp. 149-168.
- [5] MIQUELON-WEISMANN (M. F.), The convention on cybercrime: a harmonized implementation of international penal law: what prospects for procedural due process? *The John Marshall Journal of Computer & Information Law* (Winter 2005), 23, n° 2, pp. 329-361.
- [6] HOSEIN (I.), Transforming travel and border controls: Checkpoints in the open society. *Government Information Quarterly* (4th quarter 2005), 22, n° 4, pp. 594-625.
- [7] PIAZZA (P.) (ed.), Police et identification. Enjeux, pratiques et techniques. *Les Cahiers de la sécurité*, n° 56. *Institut National des Hautes Études de Sécurité*, Paris (2005).
- [8] Conseil d'État, Rapport public 2001: jurisprudence et avis de 2000. Les autorités administratives indépendantes. *La documentation française*, Paris (2001).
- [9] SCHOETTL (J.-E.), La refonte de la loi sur l'informatique, les fichiers et les libertés devant le Conseil constitutionnel. *Les petites affiches* (Aug. 2004), n° 160, pp. 8-19.
- [10] EPIC, PI, Privacy and Human Rights. An international survey of privacy laws and developments. *EPIC*, Washington (2004).
- [11] MARZOUKI (M.), Les fichiers biométriques actuels et leurs contenus in L'état des droits de l'Homme en France, édition 2006 (LDH ed.). *La Découverte*, Paris (2006), pp. 21-22.
- [12] GUILD (E.), BIGO (D.), Les pratiques quotidiennes de la coopération consulaire. *Cultures & Conflits* (Spring 2003), n° 49, pp. 96-123.
- [13] BALZACQ (T.), BIGO (D.), CARRERA (S.), GUILD (E.), Security and the Two-Level Game: The Treaty of Prüm, the EU and the Management of Threats. *CEPS*, Brussels (2006).
- [14] NOIRIEL (G.), Les pratiques policières d'identification des migrants et leurs enjeux pour l'histoire des relations de pouvoir. Contribution à une réflexion en "longue durée". *Les cahiers de la sécurité* (1st quarter 2005), n° 56, pp. 331-347.
- [15] DAVIES (S.), HOSEIN (I.), WHITLEY (E.), The identity project. An assessment of the UK Identity Cards Bill and its implications. *LSE*, London (2005).
- [16] ETZIONI (A.), Big Brother ou Big Benefits? *Les cahiers de la sécurité* (1st quarter 2005), n° 56, pp. 9-59 (A French translation of Chapter IV of Etzioni's book: *The Limits of Privacy*, Basic Books, New York (1999)).
- [17] HOSEIN (I.), Privacy as Freedom in Human Rights in the Global Information Society (Rikke Frank Jørgensen ed.). *MIT Press*, Cambridge (2006), pp. 121-147.
- [18] KERR (I. R.), GILBERT (D.), The Role of ISPs in the Investigation of Cybercrime in Information ethics in an electronic age: current issues in Africa and the world (Thomas Mendina and Johannes Brtiz, eds). *McFarland Press*, Jefferson (NC) (2004), pp. 163-172.
- [19] MARZOUKI (M.), The "Guarantee Rights" for Realizing the Rule of Law in Human Rights in the Global Information Society (Rikke Frank Jørgensen ed.). *MIT Press*, Cambridge (2006), pp. 197-218.
- [20] CRAPEAU (S.), DUBEY (G.), GUCHET (X.), La biométrie, usages et représentations. *GET/INT*, Evry (2004).

- [21] BEAUVALLET (G.), FLICHY (P.), RONAI (M.), Incorporer la protection de la vie privée dans les systèmes d'information, une alternative à la régulation par la loi ou par le marché. *Terminal* (Fall/Winter 2002-2003), n° 88, pp. 85-107
- [22] AGAMBEN (G.), Homo Sacer II. État d'exception. *Seuil*, Paris (2003). English translation entitled "State of Exception" published by The University of Chicago Press in 2005.
- [23] MARZOUKI (M.), Petite histoire de la Directive européenne sur la vie privée et les communications électroniques ou le revirement de l'Europe. *Terminal* (Fall/Winter 2002-2003), n° 88, pp. 61-83.