Data protection : a brake to police investigation?

Paper presented at the World Conference on Modern Criminal Investigation, Organised Crime and Human Rights
Sun City, South Africa, 21-25 September 1998

Introduction

Dear Sir, ladies and gentlemen,

Stating that "new technologies, especially information technologies, influence every single part of our daily life more each day" may seem commonplace. Though I remain convinced that we should constantly keep in mind that such a statement reflects a reality, whose stakes we should understand, particularly concerning public power. Even if each economic or business sector actually sees its practices or habits upset, its possibilities increased tenfold, the state police body is not outdone by that changes.

On-board computers integrated to police cars, "bugs", phone-tapping, cyber police, monitoring bracelets, databanks, monitoring cameras, identifying markings on stolen vehicles, expert's reports and DNA databanks, cross-border communication and de telecommunication networks, etc...

These various elements give the citizen the image of a police machinery that is increasingly all-powerful and omniscient. The machinery is probably the state body, important symbol of public power, whose functions and structures are among those most disturbed by technological developments.

Background

Facing the increasingly frightening idea that the society is build upon criminality, especially organised criminality, not a single citizen still imagines his police working without the different types and levels of technological innovation. The information technologies have particularly become a major question in the debate on the police. In Belgium, in the current reorganisation taking place within the police landscape, the chapter dedicated to joint computer systems and common information management clearly appears as one of the most sensitive axes in the discussions.

The boom of information and information-related technology, both at national and international levels, should bring more effectiveness and efficiency in production, processing, distribution and analysis of the information linked to delinquency (actual and potential), and therefore in the struggle against criminality. That is the case, at international level, of the Schengen Information System (CSIS, NSIS), the Information System, the Workfiles and Index system of Europol, and the Electronic Archive System (EAS), Criminal Information System (CIS) and Automated Search Facility (ASF) within Interpol, etc...

If this citizen can hardly imagine "his" police without the most sophisticated means to efficiently fight against organised criminality, this same citizen will play the role of moderator regarding the use of these means.

We have actually entered the cyber era. But the only way the anchoring of technology and the more intensive use of information can effectively operate, in the society in general, and especially in police investigation, is with the agreement of the public.
This moderation factor expresses itself through different speeches (protection of privacy, protection of

civil rights, data protection), and is more or less taken over at legal level. We will discuss this later.

I. Actors

In this short introduction, the careful listener you certainly are has already pointed out the three actors intervening in the core of my speech, as well as the stakes that I would like to highlight.

The first actor is the one whose action groups us together here, that is criminal organisation. Then comes the one many of us represent, i.e. the police. Finally, remains the one we all are, the citizen.

I.1° The criminal organisation[1]

Among the different actors of delinquency and criminality, the criminal organisation is the one which appears as the most harmful to the society, the one which most upsets the balances of which society is composed.
Though, its precise definition is such a problem that it strengthens the feeling of fear it creates. The notion of criminal organisation itself (as well as the notion of organised crime) is difficult to put in a rigid definition agreed on by all. Even if many tried to understand the global notion, the results are often vague. The reason for this is certainly to be found in the various forms, difficult to grasp, of undesirable behaviour committed by this type of organisation.
Here is the definition adopted by Interpol since 1988 : "Any association or grouping of people, indulged in continuous illegal activity, whose main objective is to make profit regardless of the borders". The terms of that definition are so general that they make it impossible to use, especially when trying to put it into material rules under the form of incrimination. Today in Belgium, the difficulties encountered in putting the notion of criminal organisation in the penal code are an excellent example. Even if our talk does not allow us to linger over the strong discussions arising from the bill on criminal organisations, still I would like to refer to it.
The Belgian government wished to insert article 342 in the Penal Code in these terms: "A criminal organisation is an association of more than two persons:
1°intending to deliberately commit crimes and offences punishable by a three-year prison sentence or a more serious sentence;
2° in order to get patrimonial advantages or influence the functioning of public authorities or public or private enterprises;
3° and using intimidation, threat, violence, fraudulent schemes or corruption or appealing to marketing structures or other to conceal or facilitate the realisation of offences."[2]

Regardless of the sometimes very critical reactions that such a suggestion could have (or still can) provoked, this definition allows the specific components of such organisation to be highlighted. First, the character of enterprise, action of a "parallel company" with a capacity of continuity in its schemes. Second, the capacity of the organisation to protect itself against the actions taken by the authority trying to stop its activities, using its power and its financial fighting spirit and its Mafia methods (aggressive counter-strategies)[3].

[1] Note that many authorities and authors confuse the two notions of criminal organisation and organised crime. Even if the link between the two is quite similar, a distinction should be made.
[2] Belgian parliamentary documents, House of Representatives, 1996-97, n°954/1, p. 3.
[3] VERBRUGGEN, Frank, *Un fer de lance trop émoussé* (A blunt spreadhead); thoughts about the bill on criminal organisations, *in* Vigiles - Revue du droit de la police, 1997, no. 2, p. 8. Note that these specific components also emerge from the 11 characteristics on which a consensus arised in 1994 and 1995 within the Working Groups on Drugs and Organised Crime of the European Union. "A group is considered to be an organised crime if at least six of the following characteristics are found: 1° co-operation of more than two persons; 2° each has its own assigned task; 3° for an extended or unspecified period of time; 4° uses one form or another of discipline and control; 5° is suspected of committing serious crime; 6° is active at international level; 7° uses violence or other means of intimidation; 8° uses commercial and business structures; 9° is involved in

These two main characteristics of the criminal organisation show its capacity to endanger democracy and State, insofar as the logic underlying research and ordinary penalty does not fit anymore[4]. Then, Criminal Law is not sufficient for authority to stop the criminality it produces, thereby running the risk of shaking democratic liberties.

Seeing this, what does our second actor think?

I.2° The police

The maintenance of law and order, the protection of the most commonly agreed values (life, body integrity, private property, etc), the enforcement of law, the prevention and suppression of offences, the protection of conditions of the exercise of fundamental liberties are so many tasks entrusted to the police in order to ensure the existence of a democratic society.

The police force is facing a situation endangering its own credibility. In matters of serious and organised criminality, recording offences committed and starting an investigation on this basis may lead to tangible results but they are often limited to rendering only the men on the front-line of crime harmless. Arresting them too quickly puts a rapid end to the investigation on the rest of the organisation for which and to the advantage of which these offences were committed. For fear of reprisals, testimonies and victims turn away from authorities and refuse to co-operate. Corruption, intimidation and violence also act within the investigation bodies themselves[5].

The failure of traditional suppression with regard to these serious forms of criminality led, and still leads the police contingent to be willing to adopt a new approach toward organised criminality. Eradication practices should evolve and new technologies represent a privileged tool in this field at two levels[6].

First, in order to improve the traditional reactive approach: the observation technologies have made a great leap forward (increasingly sophisticated imaging and sound equipment, localisation and phone-tapping, etc). The methods of localisation, collection and analysis of material clues, such as prints (finger prints or other...), micro-traces (capillary,...), etc, are developing considerably, delivering specific, sometimes highly precise, information whose recording and processing is becoming extremely powerful (such as DNA.,...).

Second, an approach rather based on bringing to light the structure and functioning of the criminal organisation, sometimes called "proactive approach", is developing in a way only possible thanks to new information technologies. Recording, analysis, transmission, cross-checking...of a huge quantity of information is now possible thanks to the development of computing and telecommunications.

---

money laundering activities; 10° influences the political scene, the media, the Administration justice authorities and/or the economy; 11° with a view to acquiring profits and/or power». See also the approach of Maurice CUSSON, *La notion de crime organisé*, *in* Criminalité organisée et ordre dans la société, Conference in Aix-en Provence (5-7 June 1996), ISPEC, Presses Universitaires d'Aix-Marseille, 1997, pp. 29 and further.

[4] VERBRUGGEN, F., op. cit., p. 8.

[5] VERBRUGGEN, F., op. cit., p. 8.

[6] "This technology is not only used in police investigation, but also in order to prevent offences. "The technologies transcending barriers traditionally obliging the police to wait until an offence is committed before questioning and predictive technologies reinforce this work. Instead of reacting to what we get, the anticipation strategies tend to reduce the risk and uncertainty. Bureaucratic organisation and modern management true to the idea of rationale (rationality), try to make control more foreseeable, safe and efficient. We leave the bare minimum to chance. Control extends to a growing number of environmental elements. To the openly hostile image of social control where authorities distinguish themselves by their uniforms and their coercive actions, comes a more veiled image, more manipulative"": Marx, G.T., *La société de sécurité maximale*, *in* Déviance et société, 1988, no. 2, p. 149.

The police demand to be able to investigate with more intrusive techniques. And numerous arguments are put forward in their support: "out of a concern for money saving and increased output of invested monies", "willing to respond effectively and radically to a currently serious problem", "in order to remain on equal terms in the struggle", "to have more correct information", "in order to anticipate new criminal acts that could arise", "considering the amazing performance offered by new technology", "because today no other alternative can bring such tangible results", or "considering that new technology should only aim at, and thus being used only towards serious criminality",...

Little by little, new tactics, improved by the recent technologies, find their place in the investigation arsenal at the disposal of the police. It is often, however, through a long procedure that these tactics become law. The "legalisation cycle", a highly complex mechanism described by Dominique Monjardet and René Lévy, often first passes through a merely praetorian practice. Second, the tactics are covered by an internal bureaucratic codification sometimes in contradiction with the current legislation in force before being moulded in a legal status.[7]

Seeing these changes, what does our third actor think?

I.3° The citizen

Sympathetic actor, while we all can find ourselves in him... the citizen has often the image of a police gathering information where they are called, that is on the spot where a crime or an offence was committed. And even if it is not that obvious to him, he also knows that the police also gather much information for preventive purposes, for security and maintenance of law and order.

The citizen hopes that this information will help to clear up the offence of which he is the victim.
As far as the general citizen is concerned, he wants to have a police able to prevent any person (or group of persons) from disturbing his enjoyment of his democratic liberties. Moreover, he is also sensitive to the sometimes great powers of policemen who execute their tasks. Putting in parallel the importance of this power and the recent technological developments mentioned in the press, the citizen sometimes becomes aware of the progress represented by such developments, but also fears the applications that could be made based on these, by the investigation bodies among others.

In addition to his wish to be protected from attacks from criminal organisations, the citizen wonders: "Am I sure that the sophisticated police methods will only be used in the strictly necessary cases? Can I be sure that the information gathered will be collected in the limited frame of the investigation? Which guarantees do I have that this information will only be used in their missions, and not for other purposes?..."

In matter of gathering, recording, processing and management of personal information by the police, the fears of the citizens should not be considered as merely imaginary. Many important scientific works, as these by Professor Flaherty on the protection of privacy in the frame of the Canadian Police Information Centre[8], clearly underlined the interrogations and problems of privacy that could arise in

[7] For more information on the cycle of legalisation of police practices, see MONJARDET, Dominique and LEVY, René, Undercover Policing in France: Elements for Description and Analysis, *in* Undercover. Police surveillance in comparative perspective, Cyrille Fijnaut and Gary T. Marx Editors, Kluwer Law International, 1995, pp. 48-49.

[8] FLAHERTY, David H., Protecting privacy in police information systems: Data protection in the Canadian Police Information Centre, *in* University of Toronto Law Journal, 1986, no. 36, pp. 116-148; See also the conclusions of SLADE, Margot and BIDDLE, Wayne, Is Big Brother to error?, *in* New York Times, 31 October 1982, section E, p. 7, quoted by BRODEUR, Jean-Paul, Droit, procédure pénale et technologie, *in* Nouvelles technologies et justice pénale - New technologies and penal justice, XXXVIII international court of criminology, under the direction of Marc LEBLANC, Pierre TREMBLAY, Alfred BLUMSTEIN, Les cahiers de recherches criminologiques, Centre International de Criminologie Comparée, Université de Montréal, 1988, pp. 557. See also the works of Marx, G.T., especially the techno-errors (sophisms) that he denounces, and that could lead to

police information management. I advise people interested to read these works. For my part I just give the example of the problems of quantity of data collected, non authorised accesses to such databanks, the often high number of persons authorised to access to these databanks, the development of practices such as data collecting, accessibility, update... in the sole hands of the police.

The worries of the citizen will be expressed at different levels, each one with a specific speech: first, the citizen will express all the reservations he feels about his future private life. This "cultural speech" will progressively be taken over within governing institutions by a "political speech" focusing on the protection of civil rights. And soon, more specific debates on certain aspects of privacy, and their rights (such as data protection), will be mentioned in a so-called "legal speech".

In other words, the specific worry of the citizen to see "his liberty of filed person" too much endangered by the liberty of the person responsible to file against him (i.e. the policeman with significant power) will progressively, through political and legal speeches, lie within more and more specific legal provisions.
First, The Right to Privacy progressively developed to the point that it now lies within the most fundamental international legal instruments (among the highest ranking according to the European Convention for Human Rights). The scope of this right extended under the pressure of "the misdeed of the benefits of progress»[9]. That's why considering the automatic management of information boom, it was necessary to examine the problem of protection of privacy from the point of view of personal data.
Consequently, a certain number of rules "lock" the collection, access, usage and processing of personal data, and organise its control... — police authorities are also submitted to these "locks". This is done at the risk of limiting them in the use of certain means of action[10].

I. 4. Equilibrium between the three actors?

In a concern of understanding and schematisation, I presented to you three typical actors, assigning to each one/several objective(s) peculiar to him, means of action peculiar to him, and specific effects that these means risk to have on one or another of them:

(actor 1)	the criminal organisation,
(objective 1)	aims at growing rich and becoming more powerful,
(means 1)	by all means, even the most violent ones,
(risk)	at the risk of destabilising democratic societies and liberties (of actor 3) as well as their basic principles;
(actor 2)	the police,
(objective 2)	aims at efficiently combatting actor 1,
(means 2)	with the most possible efficient investigation and monitoring techniques and powers,
(risk 2)	at the risk of striking a blow at the fundamental rights (such as the right to respect of privacy) of citizens (actor 3);
(actor 3)	the citizen,
(objectives 3)	- wishes to enjoy democratic liberties, and to control the action of the police (actor 2) in their means and powers,

misuse such as «Computer matching». Cf. «La société de sécurité maximale», *in* Déviance et société, 1988, no. 2, pp. 147-166.

[9] VELU, Jacques, Le droit au respect de la vie privée, Travaux de la Faculté de Droit de Namur, Presses Universitaires de Namur, 1974, p. 8.

[10] Note that, if data protection rules can limit the use of certain means of police investigation, you should not consider these rules as a negation of the efforts of the policemen in the struggle against criminality. It is rather intended to note that the means of recovery are sometimes worse than the disease itself.

- also wishes to be protected from violence of actor 1,
(means 3) via democratic institutions,
(risk 3) at the risk of limiting the margin of action of the police (actor 2).

A three-party relationship, within which the criminal organisation endangers the balance of the citizens' society, the police fight against organised crime, and finally the citizen, who on the one hand wishes that an effective struggle is lead against this type of organisation, and on the other hand refuses to be subject to a general control. We have come full circle.

The wish to be clear and schematic should not make me forget that the articulation between these three actors, presented in a rather simplistic way, operates with much flexibility. These three actors play on the same ground — the society. No one has as distinct a vision as mine. That's why there is cause to qualify my speech.

First, in the view of the worsening of organised criminality (according to numerous official documents on the subject), and regarding increasingly powerful technological possibilities, the request of police to strengthen their investigation practices seem boundless, except those ones that the citizen will always further impose in order to guarantee the respect of fundamental rights. If we are actually in presence of an equilibrium, it takes place between the last two actors (police-citizen), under the influence of the first one (criminal organisation). And it is an ever-changing equilibrium.

Then, as I said earlier, comes the citizen. It is each one of us, should we be lawyer, politician, unionist, neighbour, but also policeman or member of a criminal organisation.
The society is made of all the citizens, or group of citizens!
Therefore, this vision implies
a) if criminal organisation is really the target of police action, this organisation extends all over the society. The interplay of participation, complicity, collusion, corruption ,etc...criminal organisation may then be made of particular citizens, members of marketing or bank companies, or trade unions, politicians, etc..., and even policemen[11].
b) this reality emerging from criminal organisation forces the police to use their power and means of control over the whole of the citizens. This control, rather basic regarding the mass of citizens, strengthens in intensity and frequency as it seems to close in on its target.
c) this general control, that should be executed towards the mass of citizens with the single aim of detecting culprits, makes the "innocent citizen" feel the reality and the dangers of constraint powers and investigation techniques of policemen. Thus strengthening the need for the citizen to have a guarantee concerning the respect of his fundamental rights.
d) not forgetting, finally, that this citizen requires police contingents (and justice) able to fight effectively against criminal organisations.

Depending both on the gravity of the attacks from criminality, the investigation methods required by the policemen and the guarantees claimed by the citizen, the equilibrium between these components of the society is constantly challenged, moving, dynamic, which accentuates its fragile character all the more.

Eventually, everything is a matter of timeliness, proportionality and of subsidiarity in the determination and use of preventive and retaliatory measures by the state investigation authorities. To prevent an imbalance, the society should introduce and retain the mechanisms allowing to ensure the respect of these three principles regarding each of the lawful activities of the police.

To come back to the core theme of our speech, these very principles that were at the root of the standards governing the collection, recording, usage, communication, access, correction, storing,

[11] It is the so-called interpenetration between legal and illegal activities, that are already the subject of numerous works.

security of personal data ....and the control of the respect of these standards.

What are these standards?

II. Data protection standards

II. 1. Introduction

The national legal approaches will strongly vary to ensure to the citizen an appropriate protection in matter of data[12]. Illegal saving of personal data, processing of incorrect data, misuse or unauthorised disclosure of data... are as many aspects specifically regulated within numerous national laws on the protection of privacy. Various international instruments are even specifically dedicated to the section on privacy. I will only mention the main ones: such as the guidelines of OECD governing the protection of privacy and the cross-border flows of personal data adopted by member countries on September 23, 1980. At the European level, the Convention of the European Council for protection of people concerning computerised processing of personal data was adopted on January 28, 1981. And concerning the orientation of my speech, I want to underline also the adoption on September 17, 1987 by the European Council of Ministers of Recommendation no. R (87) 15 regulating the use of personal data in the police sector.

The steps adopted by each country, as well as at international level, concerning the protection of privacy and individual liberties have numerous common features. It is then possible to bring out certain fundamental principles that are basic components of the data protection field, such as: assigning limits to personal data collecting according to the objectives of the person in charge in this matter, limiting the use of data so that to comply to declared purposes, creating means allowing natural persons to know about the existence and contents of this data and to correct it, determining natural persons or legal entities responsible for enforcing the rules and decisions relating to protection of privacy. The laws designed to ensure protection of privacy and individual liberties linked to personal data aim at covering the successive steps of the cycle beginning with initial data collection and ending with its deletion, and ensuring all the most possible that the persons concerned will know about this procedure and will be able to participate and control it[13].

In some countries, the control mechanisms developed appear in the form of special parent bodies, such as the "authorities for data protection". In Belgium, this authority is called "Commission de la Protection de la Vie Privée" (CPVP) (Committee for Protection of Privacy). According to the Belgian law (called "Loi Vie Privée", i.e. "Privacy Law")[14], this authority has a certain number of tasks as well as powers which serve to fulfil this role.

II.2. Is the data protection brake tight?

At this stage it is time for an ultimate thinking on the following question: Are legal provisions and control mechanisms in matters of data protection a brake to police investigation? In other words, what

[12] So, certain countries have a constitution in which data protection is a human right expressly guaranteed; for other countries, only privacy is guaranteed, and data protection is considered as one of its components; for others, data protection is considered as part of other human rights: see BRUGGEMAN, W., Data protection issues in interinstitutional information exchange: the case of criminal and administrative intelligence, Europol Drugs Unit, 6th February 1998, p. 2.

[13] See OECD Guidelines governing protection of privacy and cross-border personal data flows adopted by member countries on September 23, 1980, Exposé des Motifs, p. 19.

[14] Law of December 8, 1992 on protection of privacy concerning personal data processing, Moniteur belge, March 18, 1993, pp. 5801 and further. While this law is subject to revision, I stick to the text currently in force.

is the role, the place and the impact of such a legislation and its control body in particular concerning the fragile equilibrium within the society between the upsurge of criminal activities, police reactions and citizen claims?

Giving a satisfactory answer would need a great amount of scientific research, which to my knowing has never been undertaken. However, based on my experience in this field in Belgium, I would like to let you know about the following thoughts.

The Belgian Example

The Belgian law gives the Commission in charge of its enforcement a certain number of prerogatives, such as giving notices, either on the basis of initiative or at the request of an executive or a legislative national body, on everything related to privacy concerning personal data processing. Not lingering over procedural reflections, it is however necessary to underline the fact that the notices are motivated, and that in accordance with certain provisions, it is sometimes compulsory to request a notice. In this case, the notice is published in the official national journal at the same time as the act to which it refers. It is however to be recognised that the notice given does not link the authority to which it is addressed[15].

Giving notice is probably the major activity of the Commission, while only notices contribute little by little to building case law in this matter. From 1993 (the year of progressive enforcement of the Belgian law) to 1997, the Commission has given 165 notices to all society sectors combined. A priori, it seems difficult to distinctly classify them so as to be able to count precisely those which relate to powers and police investigation methods. Nevertheless, including all notices referring to legal data management, phone-tapping, creation of databanks useful to police contingents (central recording of complaints included), to international co-operation agreements, or to the launching of a specific proactive investigation, I can count a maximum fifteen. It seems to me that it is not much considering the importance of the risk of invasion in privacy from the police investigation bodies. Still I think it necessary to underline significant changes. In the course of years, the proportion of notices given in this matter tends to increase[16]. When reading more carefully the requests for notice received by the Commission, we can foresee the new reflex of the police authorities to consult the authority for privacy protection as soon as the specified data processing involves particular risks. At the same time, we should keep in mind that the notices given have no mandatory force, but note that in practice, the moral importance of these notices is significant because they are adhered to almost every time.

An other prerogative of the Commission that we can enounce here is the control power it has on the basis of a complaint, or on initiative. To this purpose it has some powers of investigation[17]. With regard to judicial power, the Commission can also expose to the Public Ministry the offences she knows of in the exercise of its missions.

Within police contingents, controls are actually organised to ensure, with surveys, that databanks used comply with legal provisions[18]. In addition, the Commission has in the name of the citizen what law

[15] See article 29 of the Privacy Law (Loi Vie Privée).

[16] If adding the first figures I have for 1998, the increase becomes very important. On this point, we need to be balanced since Belgian judicial situation led a very important wave of reform for two years. The reorganisation projects and the legislative modifications are new opportunities to consult the Commission, and therefore one to give notices.

[17] In accordance with article 32 of the Privacy Law (Loi Vie Privée), besides resorting to experts, the Commission or its members may require communication of any useful document for their investigation, or "penetrate in any place where they have reasonable reason to suspect that an activity related to the enforcement of law is exercised".

[18] During this controls, they check not only the relevance, appropriateness, proportionality, updating of the data..., but also the similarity between the databanks actually created and those declared to the Commission. These declarations lie down in a register accessible to public, who can thus know what to expect in matters of

calls the "indirect access right"[19]. What is this right about?
The law establishes the principle according to which the citizen has the possibility to access data concerning him from the person who has it. In police matter, the lawmaker is conscious that a large access to data held by the police risks hindering the objectives pursued. Different solutions according to the country were then established. In Belgium, the solution consists of making the access right possible only through the Commission. The person who wants to access data concerning him that is in police possession should address a request to the Commission, which will exercise this access right for and on behalf of the citizen. In order to ensure total security to police work, it is also agreed that, at the end of the exercise of this right by the Commission, it merely answers to the citizen: "your data has been checked". The citizen should then be entirely confident to the Commission, because he will never know anything more.

For my part, this provision discloses the option taken by law: between "giving the citizen the control of the data managed concerning him", and "ensuring the police a larger possibility of action", police action was privileged. The citizen must not feel in control of the data that concerns him!

Of course, the Commission is still there to ensure this access right. Indeed, requests continue to flow in, and the Commission answers within satisfactory time limits using the means it has. In addition, some requests represent the possibility to exercise a larger control on police databanks.

However, in practice, we should be aware that if the quality of the information can easily be checked (to see that it is complete, updated, supported by pertinent documents), this is not the case concerning its veracity. It is hard work for the representatives of the Commission, because nothing can be disclosed to the concerned party, not even the existence of data concerning him.

We should mention here what is to be considered to be a weakness in the guarantee of the citizen's access right. When an indirect access right request is submitted to the Commission, it checks using the service(s) outlined in that request. If in the course of the check it appears that the data is obviously inappropriate, incomplete, obsolete, or even incorrect, the concerned service is required to correct it, and will systematically be controlled later. The spirit of these provisions implies that the same corrections will be required from the persons at either the origin or those acting as receivers of this data[20]. That is what I personally call the "tracing right". The evidence of such a solution however does not seem to be agreed on by the Commission. In fact no steps are taken to follow-up on incorrect data that could have been transmitted to other services. Moreover, nothing is done to get to the source of this data, while this very source is known. The Commission, while in charge of a mission of privacy protection, is legally mandated to ensure the access right for and on behalf of the citizen and refuses this "tracing right". This refusal is all the more serious, because even in this case, the citizen concerned is answered: "your data has been checked "[21].

Eventually, the example of Belgium shows that, even if some options may be open to criticism (such as the indirect access solution, non mandatory notice of the controlling body), the citizen may be very glad to see that provisions on personal data protection are adopted in the Belgian law. Such rules offer

personal data processing.

[19] See article 13 of the Privacy Law (Loi Vie Privée). It is to be noted that the royal decree on the application of this article, while provided by law, has still not been adopted to date! However, this gap did not prevent the Commission from answering requests and from exercising the indirect access right provided by this provision.

[20] Following the example of what is explicitly provided by article 93 of the Quebec law on the access to statutory bodies documents and on personal information protection, L.R.Q., chap. A-2.1. In case of rectification, a body should notify any body to which the information was transmitted.

[21] Also note the so-called "indirect access right paradox": if the body at the origin of the incorrect data is a "non police" body, that is towards which the citizen could exercise his direct access right (not going through the Commission), the Commission is legally not able to let the citizen know about that opportunity, at the risk of violating the provision obliging it not to disclose anything about the check. This paradox should urge the Commission to exercise the "tracing right".

many possibilities to ensure a respect of privacy, including against police powers of investigation requiring the processing of a huge quantity of data. These possibilities however are only of any interest if their application is effective. In this matter, the controlling body for privacy is determining.

These two examples (notice power and control power) lead us to more reserved conclusions. While we see a progressive increase in notices given in this field, it is also to be noted that they are rarely given on the Commission's initiative[22]. The reflex that seems to appear within police contingents should be subject to further study in order to determine the reasons for its appearance: actual concern for protection of privacy (progressive awareness of the society to this dimension), context for reform of police and judicial institutions, (legitimate) concern for preventing any procedural incident before the courts, fearing that lawyers could invoke the fact that the information used to sue their client does not respect the rules in data protection matters.
As far as the control power is concerned, the exercise of the indirect access right illustrates important failures in the exercise of the missions assigned to the Commission, which are all the more serious when the citizen has no means to remedy them.

Conclusion

Through these acknowledgements, I see a danger we have to address. It is the danger of "mere formalisation" of data protection in police matters. The citizen expressed a certain number of worries and requests concerning police methods and powers of investigation, particularly with regard to personal data management. The legislative solutions and procedures adopted to respond to these worries do not mean that processed and used data is correct and appropriate, but rather that the institutions only play the law game. The police authorities report, in a very formal manner**,** to control authorities in the matter. They have no report to make to the citizen. This danger becomes all the more serious when the controlling authorities do not fulfil their role of countervailing power sufficiently, sole guarantee for the citizen to see his requests met, and his rights effectively protected. In this vision, the brake is then loose.

To prevent things from going downhill, timeliness, proportionality and subsidiarity principles should again become keys ensuring a balance between powers and methods of investigation in the struggle against serious criminality and the guarantees of the respect of the citizen's fundamental rights. These principles cannot be brushed aside when the spectrum of organised criminality arises, but on the contrary should play a more important role.

It has already been ten years since, at the XXXVIII International Course on Criminology, Marx (an American professor) asked the question: "We are facing a major intellectual challenge to understand how and to what extent democratic societies are at the mercy of the destruction of liberty by supposedly non-violent technical means».[23]

---

[22] In general, the Commission seldom uses its initiative power.
[23] Marx, G.T., op. cit., 1988, no. 2, p. 149.