Essays

The GDPR and the LIBE Study on the Use of Hacking Tools by Law Enforcement Agencies

Giovanni Ziccardi*

Abstract

Digital information is, today, at the center of the cultural, social, technological and political discussions, above all with reference to its protection. In the age of big data, automated processing of information, large-scale use of algorithms and profiling systems, the risk of losing control over data and the fear of activities carried out in violation of the rights of the individuals, are very real. Over the last two years, in the context of the initiative that led to the adoption of the EU General Data Protection Regulation (the GDPR) and in some parts of a study commissioned by the Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the use of certain investigative tools by Law Enforcement agencies, data protection has been in the center of the legal debate. The GDPR places the person in the core of its protection system, and protects the individuals through the protection of their data. The LIBE Commission study, while moving from a different point of view more connected to the protection of civil rights during investigations, evaluates, at some point, the risks of individual's data processing without proper guarantees. In this essay, the two documents will be presented, trying to draw some common conclusions.

I. Introduction

Data are, today, at the center of the information society, and this is well known. That is the reason why data protection,[1] over the last twenty years, has become a central topic of political, technological, social and legal analysis.

In recent years, the national and international legislators have pointed out that, on the one hand, a strong automation process has caused the loss of control over the circulation of data and, on the other hand, it is necessary to raise the level of protection in order to guarantee the rights of the individual in the

* Professor of 'Legal Informatics', Faculty of Law, University of Milan; Coordinator of the 'Information Society Law Research Center' and of the post-graduate Course in 'Computer Crimes and Digital Investigations' of the University of Milan.

[1] For an introduction to data protection issues see, among others, M. Jori, 'Libertà di parola e protezione dei dati' *Ragion Pratica*, 109-150 (1999); P. Perri, *Protezione dei dati e nuove tecnologie. Aspetti nazionali, europei e statunitensi* (Milano: Giuffrè, 2007); Id, *Privacy, diritto e sicurezza informatica*, (Milano: Giuffrè, 2007); W. Faulkner, *Privacy. Il sogno americano: che cosa ne è stato*, (Milano: Adelphi, 2003); G. Sartor and J. Monducci eds, *Il codice in materia di protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196* (Padova: CEDAM, 2004).

technological society.[2] In the age of algorithms, artificial intelligence and big data, the individual is protected through the protection of his data, also in the States where the individual lives.[3]

In 2016, the GDPR significantly renewed the traditional protection tools, trying to adapt the data protection rules to the diffusion of social network platforms and to the practice of commercial and behavioral profiling (seen as a new frontier for online marketing).

A year later, in 2017, the LIBE Committee of the European Parliament addressed, in a very complex and innovative study, the issue of data protection and information systems during the investigations concerning the digital data of individuals (with particular regard to the suspects).

The two documents, although related to norms and areas only partially overlapping, are linked by a common thread: the idea that data, in today's society, must be considered as a fundamental good, linked to the rights of the individual. The protection of data becomes, in fact, the instrument to guarantee the protection of rights as well.

II. A Stronger Concept of 'Data Protection' in the General Data Protection Regulation of 2016

The recent GDPR clearly lays down additional obligations on private companies and public authorities that process personal data, through a new and proactive approach. The purpose of the GDPR, in fact, is to protect personal data in the information society, and is permanently applicable in all EU Countries as of 25 May 2018. It is a new, important Regulation that has impacts on daily work activities and introduces, in case of violations, a penalty system that aims to protect individual's rights and data. GDPR penalties consist of fines, possible claim for damages, and criminal penalties (if introduced by national legislations).

Fines are imposed by a Data Protection Supervisor, following investigations or claims; this Authority can, in minor cases, enact warnings, formal notices, process inhibitions or monetary fines, and it is always possible to appeal to the Court against the Data Protection Supervisor's decisions.

Particularly important for the purposes of this essay is the fact that the GDPR has considerably strengthened monetary fines, bringing them up to twenty million euros or up to four per cent of the company global turnover of the previous year. The amount of the fine depends on the nature and severity of

[2] See S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli* (Roma-Bari: Laterza, 2014).

[3] See U. Gori and S. Lisi eds, *Information warfare 2013. La protezione cibernetica delle infrastrutture nazionali* (Milano: Franco Angeli, 2014); S. Mele, *I principi strategici delle politiche di cybersecurity*, available at https://tinyurl.com/yd9j4k2w (last visited 30 June 2018); Id, *Cyber-Weapons: Legal and Strategic Aspects*, available at https://tinyurl.com/yakopzdl (last visited 30 June 2018).

the data breach, length of behavior, negligent or intentional nature of the conduct (eg knowingly ignoring a non-compliant situation), recidivism, and the presence of aggravating or mitigating factors.

Anyone who has suffered damage can claim compensation, both from the interested party (the Data Controller) and from third parties (for example, from companies that used the data); compensation can be claimed for asset damage (eg financial loss) and non-asset damage (eg loss of reputation).

The request shall be lodged with the judicial authorities against the Data Controller or Data Processor responsible for the violation, and the Data Controller (or Data Processor) is exempted from damages only proving that the harmful event is not imputable to it.

The GDPR does not directly provide for criminal penalties, but provides for the possibility of EU Countries to issue laws with criminal penalties for data processing breaches.

Concerning the individual protection, the GDPR is applicable to data relating to natural persons (in the EU, regardless of nationality and residence), including data under the control of the Controller or Processor established in the EU, data that is being processed in the EU and data processed in a public cloud (because the geographic location of the data cannot be determined). It is not applicable to data relating to legal persons or to data processed for personal (or household) use; some exceptions apply, also, in the interest of the freedom of expression and freedom of the press.

In the text of the GDPR it is possible to intend 'data protection' in many ways.

The first interpretation describes data protection as the person's sovereignty over their own personal data. The person ('data subject') must be always 'informed' (with an 'Information Statement') about the processing of the data, and has the possibility to take decisions (for example: the exercise of some rights) on the basis of this information. The statement will explain who is processing the owner's data, how data will be processed, what data is being processed, where data will be processed (geographically or in the cloud), the purpose of the processing activity and the rights that the person can exercise.

'Personal data' means any information relating to an identified or identifiable natural person, such as, for example, name/first name, surname/last name, place and date of birth, location data (home, personal or work address), identification codes (credit card, bank account), online ID (identification codes, IP address) and sensitive personal data (health status, habits, chronic diseases, hereditary diseases, diets), daily activities, membership in trade unions or political parties, sexual life and orientation and racial or ethnic origin.

The processing of personal data is forbidden unless specifically agreed by the data subject, except under special circumstances, such as the need to exercise a right related to work and social security, when life protection is threatened or

for reasons of public interest.

Special categories of personal data (sensitive data) concern political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation, racial or ethnic origin, genetic data or biometric data. At the same level of importance are data relating to criminal matters, such as criminal convictions, offenses committed, security measures related to criminal convictions (eg probation, restraining order).

A very interesting category of data are 'risky data', which imply high risks for the dignity and freedom of the person, and are subject to specific measures based on the 'impact assessment' (prior checking). Such data include profiling, mass data processing, video surveillance, geolocation, data that makes identity theft easier (eg: IP addresses, identification codes, bank account, credit card information, etc).

The processing is any operation, or set of operations, which is performed on personal data, whether or not by automated means, from collection to destruction or erasure, including consultation.

Each person shall have the right not to be subject to a decision based only on automated processing, including profiling, which produces legal effects for him or similar effects. In particular, 'profiling' in the GDPR means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person.

The Data Protection Supervisor is an independent authority, acting in full autonomy, with a mandate that has a variable duration depending on each country. The Data Protection Supervisor is responsible to supervise and ensure the application of the rules in the country, promote awareness and foster understanding of the EU Regulation, examine claims from interested parties, investigate the application of the rules, impose administrative penalties, monitor technological developments that can affect people's privacy and collaborate with the supervisory authorities of the other EU Countries.

A new professional role, the Data Protection Officer (DPO), is placed at the heart of the data protection framework: the DPO supervises data protection within the company, and should not have conflicting interests with other functions that he may be required to perform. The DPO provides advice to the Data Processor and Data Controller, supervises compliance with the regulations and company provisions regarding data processing, supervises the proper staff training and information regarding data processing obligations and cooperates with the Data Protection Supervisor. The DPO must be promptly and adequately involved in data protection issues, must be supported with necessary resources, must be independent and not receive instructions, and must report directly to top management. Moreover, he can be contacted directly by any party, can perform other tasks (if not in conflict of interest), and cannot be removed from the fulfillment of its tasks. Contact details of the DPO are communicated to the

Data Protection Supervisor and reported on all Privacy Statements.

The Officer is appointed by a Data Processor or by a Data Controller and shall be a person who meets requirements of professionalism (legal, IT and other skills and expertise), experience in the field of privacy and the ability to perform the assigned tasks. Such appointment is mandatory for public entities, while for private companies is mandatory only in specific cases (eg for companies dealing with big data such as private hospitals or insurance companies that handle large amounts of sensitive personal data).

One of the central issues of the GDPR is the security of data processing. The security system must adequately protect personal data at each stage of processing, and must protect the security of company assets that are used for processing. The aim is to prevent the risk of damage to data subjects.

The Data Controller and Data Processor must identify and adopt security measures, must provide the staff involved in processing operations with instructions and training on the topic, must check the effectiveness of the system and monitor the security system constantly and keep it updated. Staff involved in processing operations must treat the data according to the instructions received, be aware of the risks and act accordingly.

Last but not least, general protection and safety[4] of data is linked to the concept of 'accountability': it is compulsory to provide documentation and proof of the correct processing of personal data in accordance with the provisions of the GDPR, the availability, integrity and confidentiality of data, the resilience of systems and services, the use of pseudonyms or data encryption systems, the capacity to restore the system in the event of an accident and to perform efficacy tests.

The aspects of the GDPR summaried above place data protection at the center of the new legal framework. In particular, one should note the reference to 'sensitive' data, ie information that in today's society have become particularly serious and able to harm the rights of the individual, the new approach to the idea of security and accountability, and the new role of the Data Protection Officer who acts as a guardian to ensure a higher level of protection of the individual and respect for the law during data processing activities.

The purpose of the GDPR is to raise the level of information protection in a highly automated context, managed in many cases by algorithms and artificial intelligence and capable of profiling citizens with great precision.

[4] See B. Schneier, *Carry on: Sound Advice from Schneier on Security* (Indianapolis: Wiley, 2013); Id, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive* (Indianapolis: Wiley, 2012); Id, *Schneier on Security* (Indianapolis: Wiley, 2008); Id, *Secret and Lies: Digital Security in a Networked World* (Indianapolis: Wiley, 2004).

III. The LIBE Commission Study of 2017 Concerning Hacking Tools Used by Law Enforcement During Investigation Activities

In March 2017, the European Parliament (Directorate-General for Internal Policies, Policy Department, Citizens' Rights and Constitutional Affairs) published a study of over one hundred forty pages entitled 'Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices'.

It is a very complex study, urged by members of the LIBE Commission, which aims to draw several concrete legislative proposals that are appropriately preceded by a schematic (but accurate) review of the regulatory framework of six European Union States, and of three non-European states. In addition, it presents a comprehensive analysis of the ongoing political debate on the subject, and calls for a solid (and common) legal basis to regulate the phenomenon in a way that is respectful of the fundamental rights of citizens.

The underlying premise of the whole study is that the so-called 'hacking by law enforcement' (that is, the use of hacking techniques in investigative activities) is presented as a relatively new phenomenon (at least in its 'official' and 'visible' form) within the older (and traditional) political problem of finding a constant balance between security requirements and protection of data and privacy in the information society.

On the one hand, law enforcement agencies and law enforcement practitioners justify the use of such strategies (and actions) on the basis of the assertion that the use of hacking techniques has now become indispensible to bring more security, representing the only solution to the challenge that encryption has placed in the search for the elements of a crime.[5] In fact, this challenge could not be overcome by trying to systematically weaken encryption (for example, by introducing backdoors, a process that would be very complex not only from a technical point of view, but also from a 'political' one), but only by 'anticipating' the issue and penetrating directly into the information system. In simpler terms: if encryption exists, and it has been applied to data, the only two ways to overcome it are either attacking and weakening it, or by inoculating into the system a trojan that acquires data in the 'plain' and 'clear' communications environment, just before someone activates the encryption system to 'close' the information.

On the other hand, civil society actors and the scholars who are more concerned with the respect for privacy and the rights of the individual, have argued that hacking is an extremely invasive investigative tool, able to significantly

[5] See L. Lupária, *Sistema penale e criminalità informatica* (Milano: Giuffrè, 2009); Id and G. Ziccardi, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali* (Milano: Giuffrè, 2007); C. Pecorella, *Il diritto penale dell'informatica* (Padova: CEDAM, 2006); G. Pica, *Diritto penale delle tecnologie informatiche* (Torino: UTET, 1999); L. Picotti ed, *Il diritto penale dell'informatica nell'epoca di internet* (Padova: CEDAM, 2004).

impinge on fundamental rights and on the privacy of individuals. But not only that: the use of tools that should 'crack' and make systems insecure could also have a direct impact on the security of the Internet itself, and on the technology infrastructure in general. Using techniques, viruses and exploits to 'poison' the common information systems would result in a widespread insecurity and vulnerability. Very recent is the case of viruses, worms and ransomware circulating worldwide, infecting critical systems in over a hundred States, which were originally developed by enforcement or intelligence agencies: 'technological weapons' produced by States that, suddenly, began to circulate and attack the entire civil infrastructure.

The study, and this is certainly a very good point, has a highly interdisciplinary approach: firstly, it analyzes the debate at the international level and then proceeds, from a procedural standpoint, to propose possible 'legal foundations'. Finally, with a more practical approach, the relevant regulatory framework is analyzed in six European countries (France, Germany, Italy, the Netherlands, Poland and the United Kingdom) and three non-European countries (Australia, Israel and the United States of America).

The conclusions, which we will better comment in the second half of this short contibution, take the form of an interesting piece of legislative policy proposals (with accompanying recommendations). 2016 has been repeatedly indicated, among the lines of the study, as a crucial year for the subject of computer State-trojans and hacking tools: all States have shown a regulatory interest (including, ad hoc reforms) or have started drafting a legislative strategy for the foreseeable future.

The study wants to be probably an 'answer' to such a sudden 'change of course', and wants to raise the level of attention in all the operators, investigators, politicians, magistrates, lawyers and scholars dealing with human rights.[6]

The debate from which the study originated has developed, over the last few years, moving from a clear awareness of the legal challenges posed by encryption (in general), to the modern possibilities of investigation (in particular).

This awareness has given rise to a period characterized by what the study defines as the 'going dark' phenomenon: a framework in which there has been a growing lack of power in accessing data 'legally' during investigation and in effectively acquiring and examining sources that are today 'resident' on the most commonly used electronic devices, or 'constantly moving' through communication networks. Such 'darkening' of the digital sources would cause blocking of investigations, and encryption techniques are seen as one of the strongest barriers to this access.

At the same time, however, a political (and commercial) analysis reveals

[6] See M.I. Franklin, *Digital Dilemmas. Power, Resistance and the Internet* (Oxford: Oxford University Press, 2013); S. Rodotà, n 2 above; G. Ziccardi, *Resistance, Liberation Technology and Human Rights* (Berlin: Springer, 2013).

that it is still clear the intention to support strong encryption around the world, especially in products and services sold by 'big players' of the Internet, and that the ideas of 'institutional backdoors' appear unattainable.

This has led, in practice, to the use of hacking techniques during investigations to bypass encryption, by borrowing and refining the operating modes used by hackers.

At the same time, however, the study highlights clear risks for the fundamental rights to the protection of privacy and freedom of expression of thought and information: hacking techniques are, in fact, extremely invasive, especially if compared to the more traditional 'intrusive' techniques (such as interceptions, inspections, searches and seizures). Through hacking, Law Enforcement Agencies can access all data in a device or in a system. This means the management of a very large amount of data: a recent investigative activity carried out by the Dutch authority, mentioned in the study, led to the collection of seven Terabytes of data, more or less eighty-six million pages of this Journal. At the same time, the data being processed are not only significant, but are also particularly sensitive: the geographic location, movements in everyday life, communications that the subject spreads and receives, all the data stored relating to his/her life, including the most intimate ones and possibly not of interest in that specific investigation.

All these worrying aspects have not, however, prevented the political world from perceiving these tools as necessary. There was, in particular, no great public debate about the opportunity (or not) to admit similar proofs in front of a Court. They have entered slowly, in investigative everyday life, and have been used for years in many States. The discussion on the eligibility of hacking tools has never come to a real political confrontation, and has never directly involved citizens (except, perhaps, in Germany and in the United States of America, where some issues related to the matters at hand have been recalled also in the mainstream media).

A second risk is purely technological, and would ask a re-examination of the security of the Internet itself and its infrastructure: the hacking activities of Law Enforcement agencies may go beyond the targeted system, and cause damage to other unrelated systems. All in conjunction with possible ethical problems (the obligation, or not, for the Law Enforcement Agencies to report the discovery of digital weapons that they would rather prefer to reuse for investigative purposes).

There would then be a risk that involves the broader idea of territorial sovereignty: the device hacking activity could be located in another state or even 'in transit'. The same tools used to do hacking (such as a 'Remote Administration Tool') could be sold to governments or agencies with little regard for human rights, and could be used for illicit purposes (to investigate journalists, dissidents or political opponents).

In conclusion, hacking practices by Law Enforcement Agencies are seen as necessary (and admitted) in all six Countries analyzed by the Authors of the report. Four States (France, Germany, Poland and the United Kingdom) have already adopted specific rules; Italy and the Netherlands are experiencing a phase of legislative development, which, according to the study, generated a sort of 'gray zone' (hacking techniques are used by Law Enforcement Agencies, but without an express legislative framework that allows it).

The study mentions France, a State that has reported a major reform in 2011 of the Code of Criminal Procedure that has significantly increased the interception powers, reformed by Law 3 June 2016 no 731, which allowed remote access to computers and other devices. In Germany, the issue arose following a well-known decision by the Constitutional Court which established a new fundamental right to the confidentiality and integrity of computer systems (Decision BvR 370/07). Strictly speaking, German law allows the use of hacking tools both in the Criminal Procedure Code and in the Federal Crime Police Act. In Italy, use has been made, over the years, of these instruments, although not expressly governed by law. There is, however, a specific bill on the subject (with a very technical approach) and case law. In the summer of 2017, a broad reform of the whole Criminal Procedural Code included the generic possibility to use hacking tools. In Poland, regulatory reform took place in 2016 with the reform of the Police Act and the explicit provision for the possibility of hacking systems. Also the United Kingdom, since November 2016, has established a solid regulatory basis for similar practices in the Investigatory Power Act.

Such a complex legal and technological framework must inevitably provide several guarantees: the report deals with '*ex ante*' guarantees and '*ex post*' guarantees that in some States have already been implemented.

'*Ex ante*' guarantees are, in fact, the conditions under which, when and how (with what formalities) such tools can be used. In this case, particular attention is pad to the fact that the use must be proportionate and necessary, that there must be a Court decision as a legal basis (the report usually defines it as a 'judicial authorization'), and that there must be guarantees of duration, purpose and the limitation of such investigative techniques to a certain type of crime.

'*Ex post*' guarantees are related to the presence of a supervisor, the ability to view log files and remedies to be put in place in case of incorrect use of such tools (resulting in compensation for damages or compulsory mitigation of harmful effects).

Concerning the limitation on the use of such tools based on the crime or the maximum duration of the prison term for specific offenses, all six States restrict the use of hacking tools on the basis of the severity of the crime. In some States, legislation provides for a specific list of crimes where hacking is permitted. In other States, however, the possibility of the use of such tools is provided only for those crimes that are punished with a high maximum of prison's years (in this

case, the study records significant differences between the various States). Some States, moreover, limit the timeframe in which hacking activities can be carried out: from one month (France and the Netherlands) to six months (UK), although time extensions are allowed.

Such '*ex ante*' guarantees, coupled with additional, specific '*ex-post*' guarantees (such as target notification of illegal hacking practices, log file keeping of all activities, and activation of audit and control systems) should ensure a balanced and as fair as possible picture of everyone's rights.

IV. Conclusions

There are some aspects that link the two documents that we have described above, and which allow us to draw some interesting considerations on the treatment and protection of data in today's society.

First of all, the idea behind the GDPR is to address matters regarding personal data in a 'more modern' way which is more closely linked to the era of smartphones, fitness bracelets,[7] social networks, profiling algorithms, data mining activities[8] and automated decisions. Secondly, in addition to the more traditional concept of personal data, which remains, the focus is on data that are connected to the electronic life of the individuals and their identity on social networks and that deserve, today, the same level of protection.

At the same time, the LIBE document highlights the level of dissemination that data have achieved in our society – data that are controlling the citizens,[9] that crosses the boundaries and that requires, in its treatment, a necessary cooperation between public and private, especially in case of computer crimes[10] or big data breaches and security flaws.

[7] See E. Germani and L. Ferola, 'Il wearable computing e gli orizzonti futuri della privacy' *Il Diritto dell'Informazione e dell'Informatica*, 75-101 (2014).

[8] D.J. Solove, 'Data Mining and the Security-Liberty Debate' 75 *The University of Chicago Law Review*, 343-362 (2008), also available at https://tinyurl.com/6p8ark (last visited 30 June 2018).

[9] Concerning the use of technologies as a control tool, see D. Campbell, *Il mondo sotto sorveglianza. Echelon e lo spionaggio elettronico globale* (Milano: Eléuthera, 2003); D. Lyon, *L'occhio elettronico. Privacy e filosofia della sorveglianza* (Milano: Feltrinelli, 1997); Id, *La società sorvegliata. Tecnologie di controllo della vita quotidiana* (Milano: Feltrinelli, 2002); Id, *Massima sicurezza. Sorveglianza e "guerra al terrorismo"* (Milano: Raffaello Cortina, 2005).

[10] See L. Lupária, n 5 above; C. Pecorella, n 5 above; G. Pica, n 5 above; L. Picotti, n 5 above.