Privacy and security: two sides of the same coin. Looking for a balanced view

LAURA FEROLA
PhD in International Law and Human Rights, Official, The Garante per la Protezione dei Dati Personali (Italian Data Protection Authority)

Introduction: Moving Towards an "Orwellian "Society?

Europe is facing unprecedented threats to its public security: recent terrorist attacks in several Member States as well as the unstable situation in the Middle East showed the necessity to tackle these phenomena in a concerted and meaningful way.

It is evident that terrorism is not a regional problem, but a global one and as such it requires a global response: although competence over national security and criminal matters is strictly reserved for national sovereignty, the complex cross-border methods adopted by terrorists have rendered it imperative to co-operate also with other countries and develop sophisticated investigations, especially on the Internet.

Surveillance activities from intelligence services become more efficient and, in parallel, more intrusive for citizens: it is a matter of fact that the scale of data processing – as made possible through cloud computing, big data analytics and electronic mass surveillance techniques – is also unprecedented. Intelligence services process large amounts of personal data on a daily basis, share these information extensively with other services in and outside the European Union.

Indeed, the Snowden revelations disclosed the existence of many different surveillance programmes run by intelligence services, which

are able to collect data about virtually everyone.[1]

In this light, security comes at a cost.

Surveillance programmes result into large-scale controls that may in turn give rise to secret, massive and indiscriminate surveillance of everybody with unjustified limitations on citizens' privacy.[2]

Many of these programmes seem to be aimed at the bulk collection of personal data from various online sources, do not distinguish between suspected and non-suspected individuals and, in case of communication, concern both content and traffic data.

The way intelligence services collect and make use of data on our day-to-day communications as well as the content of those communications underlines the need to set limits on the scale of surveillance; this has been brought into the debate with regard to their interference in individuals' privacy.[3]

---

[1] Edward Joseph Snowden is a computer professional, former Central Intelligence Agency (CIA) employee, and former contractor for the US Government; in 2013, he presumably copied classified information from the United States National Security Agency (NSA) and United Kingdom Government Communications Headquarters (GCHQ) for public disclosure without prior authorization. The information revealed numerous global surveillance programs, many run by the NSA with the cooperation of telecommunication companies and European governments within the framework of the top-secret PRISM programme.

[2] See Article 29 Data Protection Working Party, 'Working Document on surveillance of electronic communications for intelligence and national security purposes', WP 228, adopted on 5 December 2014, http://ec.europa.eu/justice/data- protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf. This Working Party was set up under Art. 29 of Directive 95/46/EC (see *infra*); it is an independent European advisory body on data protection and privacy. It is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.

[3] Privacy originates from the traditional "right to be alone", i.e. the individuals' right to be not submitted to any unlawful interference by a public authority or other individuals. This "*jus solitudeinis*" differs from other fundamental rights, substantially unchanged in time, because it was enriched with other elements progres-

The right to privacy and to the protection of personal data is a fundamental right enshrined in several international instruments (art. 12 and 29 of the Universal Declaration of Human Rights; art. 17 of the International Covenant on Civil and Political Rights; art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms the European Convention on Human rights) as well as at European level (art. 7 and 8 of the EU Charter of Fundamental Rights; art. 16 of the Treaty on the Functioning of the European Union) and in national legislations.

EU Member States may adopt legislative rules to restrict privacy and data protection rights: according to Directive 95/46/EC,[4] governments may adopt measures that restrict this fundamental right to safeguard national security and democratic order, but these measure may only be lawful if they are strictly necessary and proportionate in a de-

sively. Privacy is included in the broader right to protection of personal data, *i.e.* the right that personal data undergoing processing shall be processed lawfully and fairly; collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes; accurate and, when necessary, kept up to date.

[4] According to art. 13, par. 1, of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (in *O.J.E.U.* L 281 1995, p. 31), restrictions are admitted only if these are necessary to safeguard, among others, (a) national security; (b) defense; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the EU; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); or (g) the protection of the data subject or of the rights and freedoms of others. The same principles are stated by art. 23 of the so-called General Data Protection Regulation, which is going to repeal Directive 95/46/EC with effect from 25 May 2018 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in *O.J.E.U.* 2016 L 119, p. 1).

mocratic society; in addition, respecting the rule of law is a fundamental pre-requisite for the lawfulness and legitimacy of any such measures.[5]

Fighting crime and terrorism are clearly legitimate objectives, but data protection is a democratic value and it can reinforce democracy in the digital age:[6] security and privacy are the two sides of the same coin.

A balanced reconciliation of these two components must be reached.

The Approach of Courts to the Investigative Potentialities Offered by New Technologies

The terrorist attacks in Europe altered the traditional equilibrium reached between privacy and security: as underlined in the well-known judgment on EU data retention Directive.[7] sacrificing the right

[5] For an overview on this issue at Member States' level, see European Union Agency for Fundamental Rights, *Fundamental Rights Report 2016*, Luxembourg, 2016, p. 117, which summarises and analyses major developments the fundamental rights field – including information society, privacy and data protection – in the European Union during 2015.

[6] See Data protection as a bulwark for digital democracy, Keynote speech at the 6th International e-Democracy 2015 Conference on Citizen rights in the world of the new computing paradigms Athens (by recorded message), 10 December 2015, by Giovanni Buttarelli, European Data Protection Supervisor, https://secure. edps. europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-12-10_eDemocracy_EN.pdf. The European Data Protection Supervisor (EDPS) is an independent supervisory authority, with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.

[7] CJUE, *Digital Rights Ireland ltd vs. Minister for Communications, Marine and Natural Resources and others and Kärntner Landesregierung*, joined cases C-293/12 and C-594/12, judgement of 8 April 2014. The Court has declared the incompatibility with art. 8 and 7 of EU Charter of fundamental rights of European Data Retention Directive 2006/24/EC. Although the above mentioned Directive only allowed the storing of external data related to communications and pursuant to a legitimate objective (the fight against serious crime), it nonetheless entailed a disproportionate

to the inviolability of private communications constitutes a restriction on that fundamental right, which is permissible only if it is proportionate to the pursued goal, when there are very important reasons imposed by the criminal investigation linked to criminal proceedings and it is based on fundamental guarantees.[8]

The ECHR also found that some national rules did not provide sufficient safeguards to avoid misuse and subjected virtually everyone to surveillance. In a case concerning a Hungarian law on antiterrorist surveillance, introduced in 2011, the Court found a violation of art. 8 of the European Convention on Human Rights.[9] The Court held that the law, enabling the Government to intercept masses of data easily by

interference with the fundamental right to respect for private life and personal data. The Court pointed at the lack of clear and precise rules aimed at limiting the interference with those rights to what was strictly necessary in order to achieve the Directive's objective. The Directive applied without distinction to all individuals, electronic means of communications and traffic data, and it did not contain objective criteria aimed at defining who could access stored data or the length of the retention within the range of 6-24 months. Moreover access to data kept by national authorities was not subject to prior review by a court or a national independent body, nor were there sufficient guarantees against the risk of misuse or illegal use of the data. By adopting Directive 2006/24/EC, the EU legislature exceeded the limits imposed by compliance with the principle of proportionality in the light of articles 7, 8 and 52(1) of the EU Charter on Human rights. Cf. specially para. 52 , 54, 65, 47.

[8] See 'Computers, privacy & data protection, 2015 Data protection on the move', concluding remarks by Giovanni Buttarelli, European Data Protection Supervisor, Brussels, 23 January 2015, https://secure.edps.europa.eu/EDPSWEB / webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-01-23 _CPDP_concluding_remarks_GB_EN.pdf.

[9] ECHR, Fourth section, *Case of Szabó and Vissy v. Hungary*, Application no. 37138/14, 12 January 2016. See also ECHR, *Roman Zackarov v. Russia*, Application n. 47143/06, 4 December 2015: with this judgment, the Grand Chamber stated that "since the implantation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an *unfettered power*". More recently, see *Big Brother Watch et others v. United Kingdom*, Application no. 58170/13 (to be decided).

means of new technologies, foresaw that the ordering of such measures could be adopted entirely within the realm of the executive, and without an assessment of whether interception of communication was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.

This is the direction followed by the courts in several States as well, which gave a new dimension to the balance between security and privacy, justice and intelligence services – thus confirming that data protection has come to play a pivotal role in the digital society.

The Portuguese Constitutional Court declared unconstitutional a norm contained in an Assembly of the Republic Decree approving the Portuguese Republic's Intelligence System.[10] The norm would have allowed intelligence officers from the security services to access "traffic data" under certain conditions, to pursue goals linked to the prevention of phenomena like terrorism, espionage, sabotage and highly organised crime.

The proposal did not envisage direct access to the contents of communications (written or voice), as it rather allowed obtaining an authorisation to request the entities that are legitimately responsible for processing such data (base, location and traffic) to enable access to them.

According to the Court, access to data on actual or attempted communications can undermine the fundamental rights of the persons involved in the individual communication. Even without access to the content, the cross-referencing of traffic data can provide a profile of the person in question and it may disclose aspects of people's private lives.

Interlocutors are entitled not to have third parties intervene in their communications. States and communications providers are required to guarantee the integrity and confidentiality of communications systems,

[10] Tribunal Constitucional, *Acórdão n.º 403/2015, Processo n.º 773/15, 27 de agosto de 2015, Pronunciamento pela inconstitucionalidade da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República que Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa*, http://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

ensuring that communication at a distance between private parties takes place as though they were face-to-face.

If public authorities should be allowed to intrude into telecommunications in the cases provided for in criminal procedural law, the risk is that it would imply both expanding the scope of application of the restriction on the right to inviolability, and reducing the guarantee that only a judge can authorise such interventions by relegating the control of acts that affect fundamental rights to a merely administrative entity. Exceptions referred to in the constitutional precept are limited to matters regarding criminal proceedings. This is the only restriction on the right to the inviolability of communications which the Constitution authorises, and there can be no other interpretation that would make it possible to extend the restriction for other purposes. The norm in question did not do this, and this was the reason why the Court pronounced the norm before it unconstitutional.

The same stance was taken by the Italian Supreme Court, which declared it unlawful to perform interceptions by installing computer worms in a smart phone in order to activate its camera remotely without the owner's knowledge;[11] as a consequence, admissibility of the relevant interceptions was ruled out. According to the Court, that investigative technique would enable, in breach of the Italian Constitution and the criminal procedural code, a total control of the suspected person which would be so pervasive and unlimited as to be unacceptable in a democratic order.

[11] Corte di Cassazione, sez. VI Penale, sentenza 26 maggio – 26 giugno 2015, n. 27100, http://www.italgiure.giustizia.it/sncass/. This is the highest (third-instance) judicial Court and is expected to ensure the exact observance and uniform interpretation of the law, the unity of the national law, and compliance with the limits of the various jurisdictions. One of the key features of its mission is its legally unifying function, essentially aimed at ensuring certainty in the interpretation of the law. Thereafter, the Italian Supreme Court admitted exceptionality the installation of computer worms in a smart phone to counteract organized crime (see Cassazione Penale, Sezioni Unite, 1 luglio 2016, ud. 28 aprile 2016, n. 26889; see also sez. VI Penale, sentenza n. 27404/16, lodged on 4 July 2016).

It is towards this 'new deal' that the Supreme Court of the United States is also moving, as it extended the guarantees for personal liberties to data stored in cell phones.[12]

The Court, moving from two different cases (illegal trafficking of weapons and drugs), stated that where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant. This same principle applies also before searching information stored or accessible on cell phones, "*which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy*".

Expectations of privacy may not be reduced by the arrest without any reason: inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself. This may make sense as applied to physical items, but more substantial privacy interests are at stake when digital data is involved.

The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. One of the most notable distinguishing features of modern cell phones is their immense storage capacity.

Therefore, a warrant ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.

According to the Court, in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the Fourth Amendment's warrant requirement.[13]

---

[12] Supreme Court of the United States, *Riley v. California*, 573 U.S. (2014), decided June 25, 2014, http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

[13] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

A Key Case: Collection of PNR (Passenger Name Records)

One of the methods considered useful for fighting terrorism is the collection of the so-called PNR (passenger name records) data and an EU Directive was adopted to regulate the use of these data.[14]

The Directive will oblige airlines to hand EU countries their passengers' data in order to help the authorities to prevent, detect, investigate and prosecute terrorist offences and serious crime. A single list of offences has been agreed upon, including terrorism, trafficking in human beings, participation in a criminal organisation, cybercrime, child pornography, and trafficking in weapons, ammunition and explosives.

It will provide for the transfer by air carriers to EU Member States "Passenger Information Units" (PIUs) of PNR data of passengers of "extra-EU flights" (i.e. from a third country to an EU Member State or vice-versa). It will allow, but not oblige, Member States to apply its provisions also to "intra-EU flights" (i.e. from an EU Member State to one or more EU MS): in that case, if a Member State wishes to apply this Directive to intra-EU flights, it shall give notice in writing to the Commission to that end (art. 2).

Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action only for the specific purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime (art. 7).

To that end, the PNR data provided by the air carriers to the national PIUs is to be retained for a period of five years. For the first six months, the data will be "unmasked", i.e. will include personal identifying information. The data will then have to be "masked out" for the remaining four and a half years (art. 12). It should be recalled that the

[14] See Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', in *O.J.E.U.* 2016 L 119, p. 132.

5-year term does not apply to any PNR data transmitted by the PIUs to national competent authorities; in that case, the retention period of the data is the one provided for under the applicable national law.

Depersonalising data through "masking out" means rendering certain data elements invisible to a user, such as name(s), including the names of other passengers on PNR and number of travellers on PNR travelling together, address and contact information, etc. (*i.e.* data elements that could serve to directly identify the passenger to whom the PNR data relate).

National PIUs are obliged to appoint a data protection officer responsible for monitoring the processing of PNR data and implementing the related safeguards, and to act as a single point of contact on all issues relating to the processing of the passengers' PNR data, duties and powers for the national supervisory authority, which will be in charge of checking the lawfulness of the data processing and conduct investigations (art. 5). Access to the full PNR data set, which enables users to immediately identify the data subject, should be granted only under very strict and limited conditions after the initial six-months retention period (art. 12).

All processing of PNR data should be logged or documented, and passengers should be clearly and precisely informed about the collection of PNR data and their rights (art. 13).

It must pay special attention to compliance with personal data protection standards, the necessity and proportionality of collecting and processing PNR data for each of the stated purposes, the length of the data retention period, and also the effectiveness of the sharing of data between the Member States. Therefore, national supervisory authorities shall advise on and monitor the application of the Directive, with a view to protecting fundamental rights in relation to the processing of personal data (art. 15).

The EU PNR Directive will be reviewed two years after its transposition into national laws (art. 19).

It is a matter of fact that an PNR scheme programme would be the first large-scale and indiscriminate collection of personal data within

the EU, since it is likely to cover at least all flights to and from its Member States and may also involve intra MSs and/or domestic flights.[15]

It is estimated that the system would concern more than 300 million non-suspect passengers potentially targeted by the EU PNR Directive: it would apply to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

It is interesting to quote some critical observations from the EDPS on the above mentioned Directive;[16] information about the perpetrators

[15] It must be borne in mind that the EU has already signed agreements allowing EU carriers to transfer PNR data to the United States, Australia and Canada. In June 2015, the Council adopted a decision authorising the opening of negotiations for an agreement with Mexico. See: 'Agreement between the United States of America and the European Union on the use and transfer of the passenger name records to the United States Department of Homeland security' (in *O.J.E.U.* 2012 L 215, p. 5); 'Agreement between the European Community and the Government of Canada on the processing of the Advance Passenger Information and Passenger Name Record data' (in *O.J.E.U*. 2006 L 82, p. 15); 'Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service' (in *O.J.E.U*. 2012 L 186, p. 4).

[16] For further details, see EDPS, 'Opinion 5/2015, Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', *Brussels*, 24 September 2015, in https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf. See also Article 29 Data Protection Working Party, 'Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', WP 181, adopted on 5 April 2011, in http://ec.europa.eu/ justice/policies/privacy/docs/wpdocs/2011/wp181_en.pdf;id., 'Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries', WP 178, adopted on 12 November 2010, in http://ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2010/wp178_en.pdf

was already available through airlines, national authorities and databases for border control (SIS, VIS etc.) or Advanced Passenger Information (API), therefore more targeted measures should be considered such as monitoring known suspects, which would be more effective than profiling all travellers.

In addition, the use of dynamic, human intelligence should be encouraged rather than the fatally flawed automated intelligence.

Such investigative approaches as well as more selective and less intrusive surveillance measures based on targeted categories of flights, passengers or countries would be more legally robust and useful:[17] for instance, the Directive should be targeted at specific third countries or at itineraries of types of travellers assessed objectively as indicating a greater risk.

In addition, the EU PNR being negotiated is a set of different, separate national PNR systems and does not provide for the coordination, collection and analysis of PNR data at EU level or for the mandatory exchange of information by Member States. The text simply obliges each Member State to implement its own national PNR scheme, following the principles laid down in the Directive.[18]

---

[17] "The EU needs to justify why any and indiscriminate collection of data of individuals is really needed [see para 17 of C-293/12 and C-594/12 judgment], and why – as many are arguing in the case of PNR – that measure is urgently needed now" considering also that "Recent public statements from public prosecutors with a solid counter-terrorism background highlighted their favour for more targeted approaches by investing more resources on dynamic intelligence instead of delegating the response to passive large scale databases we are unable to fully analyse", as it was underlined by Giovanni Buttarelli, European Data Protection Supervisor, in *Counter-terrorism, De-Radicalisation and Foreign Fighters, Joint debate during the extraordinary meeting of the LIBE Committee*, European Parliament, Brussels, 27 January 2015.

[18] Surprisingly, the Directive states expressly that it "is without prejudice to the applicability of Directive 95/46/EC" (art. 13), although the latter is going to be repealed by the GDPR with effect from 2018. Similarly, the Directive foresees that transfers of PNR data by Member States to third countries should be permitted only on a case-by-case basis and in full compliance with the provisions laid down

Concluding Remarks

Enhancing security needs surveillance and privacy-affecting technology, in order to improve specific criminal investigations or prosecutions, that's und oubtable.

Technological progress has increased the possibilities of intrusion; however, rules may assess, on the one hand, the degree to which investigative tools intrude upon an individual's privacy and, on the other, the degree to which they are needed for the promotion of legitimate governmental interests.

The same tools (*e.g.* Internet, smart phones, etc.) that terrorists and criminals are using to hide their nefarious activities are those that everyday citizens rely on to safely shop online, communicate with friends and family, and run their businesses. Since it is expected that terrorists and criminals, more in general, conceal their messages through end-to-end encryption, secure apps and other tradecraft or hidden tactics to avoid getting caught and creating a much broader public safety crisis, more sophisticated tools can be adopted to counteract criminal behaviours. But if those tools are used without an appropriate selection, the risk is that also the man in the street is monitored.

Protecting the rights to privacy and data protection, as well as cyber security may converge onto the same objective: safeguarding democratic liberties.[19] Terrorism must be tackled using democratic means: in

---

by Member States pursuant to Framework Decision 2008/977/JHA (art. 11), despite the fact that the mentioned Framework Decision is repealed, with effect from 6 May 2018, by the Directive 2016/680regarding the processing of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences (see below).

[19] For a deeper analysis of problems linked to privacy and security, see VV. AA., *La società sorvegliata. I nuovi confini della libertà – Atti del convegno del 28 gennaio 2016 organizzato dal Garante per la protezione dei dati personali in occasione della Giornata europea per la protezione dei dati personali 2016*, Rome, 2016, p. 173; G. Valkenburg,'*Privacy versus security: problems and possibilities for the trade-off model'*, inS. Gutwirth, R. Leenes & P. de Hert (eds.), *Reforming European Data Protection Law*, Dordrecht-Hidelberg, 2015, p. 253; M. Leese, *Privacy and Security – On the Evo-*

a democratic order, *habeas corpus* may not live apart from *habeas data.*

National security must not become an excuse for disproportionate processing of personal data such as in the case of intrusive surveillance tools, and it is important to focus on sustainable and long term policies.

Sustainability also means being true to our values in terms of fundamental rights and freedoms, and States must ensure full compliance with their obligations under international human rights law in a balanced way.[20]

There is no security without privacy"[21] and we need a standard which is centred on the rights of the individual.

---

lution of a European Conflict, *ibid*., p. 253; K. Irion, *'Accountability unchained: bulk data retention, preemptive surveillance, and transatlantic data protection'*, in M. Rotenberg, J. Scott & J. Horwitz (eds.), *Privacy in the Modern Age: The search for solutions*, New York, 2015, p. 78; Y. Jin Park, *A Broken System of Self-Regulation of Privacy Online? Surveillance, Control, and Limits of User Features in U.S. Websites*, in Policy & Internet, 4, 2014, p. 360; G. Busia, 'Le frontiere della privacy in Internet. La nuova corsa all'oro per i dati personali', in Pollicino, E. Bertolini & V. Lubello (eds.), *Internet: regole e tutela dei diritti fondamentali*, Milano, 2013, p. 14; D. Bigo*et al*., *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, *Study for the European Parliament*, Brussels, 2013, in http://www.europarl.europa.eu/Reg Data/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf; V. Mayer - Schönberger-K. Cukier, *Big Data: A revolution that will transform how we live*, *work, and think*, 2013, p. 242.

[20] "Solving this problem requires establishing a dialogue that takes fuller account of technological limitations, investigative tools and legal needs. As a result, digital innovations present us with a paradox. We are no longer simply weighing the costs and benefits of "privacy vs. security" but rather 'security vs. security'. We must never lose sight of our core democratic values and we cannot weaken Internet privacy for everyone". In that sense, M. McCaul (chairman of the U.S. House Homeland Security Committee) and M. Warner (member of the U.S. Senate's Banking, Finance and Intelligence committees), 'How to unite privacy and security – before the next terrorist attack', *The Washington Post*, December 27, 2015, https://www.washingtonpost.com/opinions/how-to-unite-privacy-and-security--before-the-next-terrorist-attack/2015/12/27/628537c4-a9b3-11e5-9b92-dea7cd4b1a4d_story.html

[21] These words belong to B. Schneier, *Security vs. Privacy*, 2008, in https://www.schneier.com/blog/archives/2008/01/security_vs_pri.html

Therefore, it is important to affirm that the same rights that people have offline must also be protected online, in particular the right to privacy. States must be called on to protect these rights on all digital platforms.[22]

It is essential, at European level, to have a clear set of criteria that law enforcement and national security must respect when they affect the personal sphere of every individual by pursuing activities such as the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.[23]

To meet the requirements stated by the CJUE in the above-mentioned data retention judgement, every instrument needs to lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in articles 7 and 8 of the Charter of Fundamental Rights of the EU and the scope and application of the measures in question, and imposing minimum safeguards to provide sufficient guarantees to effectively protect data subjects' rights.[24]

A selective, case-by-case approach rather than a massive, pervasive,

---

[22] There is a broad consensus in both doctrine and case law that traffic data should be included in the concept of communications that are constitutionally relevant to the prohibition on intrusion. In that sense see, UN, *The right to privacy in the digital age*, Resolution no. 69/166 adopted by the General Assembly on 18 December 2014, A/RES/69/166.

[23] Criteria established by the adoption of the 'Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA', in *O.J.E.U*. 2016 L 119, p. 89.

[24] See EDPS, Opinion 8/2015, *Dissemination and Use of Intrusive Surveillance Technologies*, 10 December 2015, in https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-12-15_Intrusive_surveillance_EN.pdf. Another interesting source of toolkits for policymakers to help them develop innovative solutions to data protection challenges may be founded in *The EDPS Strategy, Leading by example, 2015-2019*, Luxembourg, 2015, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Publications/Strategy 2015.

non-targeted and indiscriminate approach would better work in order to guarantee an efficient action according to the different nature of the crime: a correct approach should properly distinguish between specific requirements of national security and the necessity to counteract terrorism and other criminal offences typically committed in the Internet (paedophilia, phishing, illegal trafficking, etc.).[25]

Such an approach should rule out the appropriateness of implementing other, less intrusive options, respecting the privacy-by-design principle (*i.e.* embedding data protection safeguards in the technology in the design phase) as well as the privacy-by-default one (*i.e.* ensuring that the default settings of technology are compliant with data protection, in the absence of specific users´ choices), both foreseen by art. 25 of the General Data Protection Regulation 2016/679/EU (hereinafter GDPR) and art. 20 of the Directive 2016/680/EU.

Hence the importance of the common rules established at European level by means of the above mentioned instruments.[26] in order to assure that any processing of personal data is lawful, fair and transparent in relation to the natural persons concerned, and only processed for specific purposes laid down by law. As it was underlined in the above named European acts (see specially art. 4 and 13 of the Directive 2016/680/EU; art. 6 of the GDPR 2016/679/EU), this does not in itself prevent the law-enforcement authorities from carrying out activities such as covert investigations or video surveillance:

---

[25] "Effectiveness isn't the only question that must be considered, and even an otherwise robust policy must be balanced against its adverse impact on other values. But effectiveness is a threshold question … If we do not first ask what is working and if anything is likely to work better, adjustments in our security policies are likely to be both ineffective and corrosive of civil liberties and other principles of democratic governance", as it was stressed by J. Dempsey, 'Restricting encryption is a short-term solution to a long-term problem', *The Washington Post*, December 18, 2015, https://www.washingtonpost.com/news/in-theory/wp/2015/12/18/restricting-encryption-is-a-short-term-solution-to-a-long-term-problem/

[26] Similar provisions are contained also in *Convention No. 181 for the Protection of Individuals with regard to Automatic Processing of Personal Data*, adopted by the Council of Europe on 28 January 1981.

Such activities can be done for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as long as they are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned (recital 26 of the Directive 2016/680/EU).[27]

In this particular field, also transparency is important, not hiding behind opaque or misleading 'privacy policies': explaining who is responsible for collecting and using personal information, why they are doing it, purposes of and legal basis for the processing, how long they will keep it, with whom they intend to share the information, and give individuals up-to-date, meaningful, rights to access and to information about data processing (*e.g.* the existence of the right to request from the controller rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, as well as the right to lodge a complaint with a national supervisory authority). In particular, if personal data are processed in the course of a criminal investigation and court proceedings in criminal matters, it is essential to provide – when, of course, it does not create a prejudice to investigations or procedures – the exercise of the right to information, access to and rectification or erasure of personal data, and that restriction of processing is carried out in accordance with national rules on judicial proceedings (see art. 14 and 15 of the Directive 2016/ 680/EU[28]).

[27] This, also in accordance with articles 51-54 of the Charter of Fundamental Rights of the EU and art. 8, par. 2, of the Convention for the Protection of Human Rights and Fundamental Freedoms.

[28] Indeed the Directive 2016/680/EU emphasized (recital 44) that "legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data to the extent that and as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to avoid obstructing official or legal inquiries, investigations or procedures, to avoid prejudicing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

From a different perspective, another important safeguard, when sharing personal information with third countries, consists in the obligation for the transmitting authority to check that the data processing is lawful in those countries (in particular, under the conditions set forth in art. 35 of Directive 680/2016/EU).[29]

Privacy is a fundamental right and we cannot have security by undermining it: this is the real challenge to meet for implementing, in the next future, efficient actions to protect democracy and freedom in the digital era.[30]

---

penalties, to protect public security or national security, or to protect the rights and freedoms of others. The controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted".

[29] It should be checked that the request is compliant with national legislation and international agreements, that it is made for specified, explicit and legitimate purposes and that the data will be processed only for the purpose mentioned in the agreement, that only data that is accurate, complete and updated, as well as adequate, relevant and not excessive in relation to this purpose is transmitted; that any further processing for a different purpose, transmission to another authority, agency or body, is authorized by the sending State and subject to strict conditions; that the data will not be retained longer than necessary for the purpose pursued; and finally, that an independent supervisory authority is responsible for checking that these requirements were respected in both the transmitting and the receiving Party.

[30] Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, WP 215, adopted on 10 April 2014, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf; and *Working Document on surveillance of electronic communications for intelligence and national security purposes*, WP 228, adopted on 5 December 2014, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf. See also *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, WP 186, adopted on 13 June 2011, in http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp186_en.pdf.