Recent developments in the recognition of digital privacy as a human right[1]

Valentina Maria Ariemme[2]

1. New frontiers for the right to privacy in the twenty-first century. The concept of digital privacy

The recognition of privacy as a fundamental human right dates back several decades, along with the recognition of the need to safeguard it against external violation[3]. However, privacy rights attracted renewed attention in 2013, when the leaking of sensitive data, international espionage, and the unauthorized disclosure of information resulted in extensive media coverage and political controversy in a number of countries around the world.

These developments highlighted the new risks to which personal privacy is exposed in the Internet era and gave rise to a powerful response in terms of public opinion and at many political levels, both national and international.

One of the most important debates took place within the UN, with an exchange of views between the High Commissioner for Human Rights (Navanethem Pillay), and the UN Member States, international and regional organizations, and human rights organizations[4].

---

[1] How to quote this article: V. M. Ariemme, Recent developments in the recognition of digital privacy as a human right, in *European Tax Studies*, 2014, No. 2, (www.seast.it/magazine), pp. 78-83.

[2] Valentina Maria Ariemme, PhD candidate in European Tax Law at European School of Advanced Tax Studies – Alma Mater Studiorum, University of Bologna, Italy.

[3] The Universal Declaration of Human Rights, proclaimed by the General Assembly of United Nations (UN) on 10 December 1948, Article 12, provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation". Again, still from the UN, but two decades later (December 1966), the International Covenant on Civil and Political Rights, Article 17 par. 1, states the same concept in almost the same words, adding, at paragraph 2, that: "Everyone has the right to the protection of the law against such interference or attacks".
See the United Nations website for the full text of the Declaration and the website of the UN High Commissioner for Human Rights for the full text of the Covenant.

[4] All relevant documents are to be found on the UN website, www.un.org (see, in particular, the resolution adopted by the General Assembly on 18 December, n. 68/167. The right to privacy in the digital age) and on the website of the High Commissioner for Human Rights. See also, on human rights safeguards, the Human Rights Watch website.

The final report from the Commissioner was published on 30 June 2014 providing an overview of the main issues.

The starting point of the report is that the development and dissemination of Internet technologies: *"[….] offer the promise of improved enjoyment of human rights". However, at the same time "[…] in the digital era, communication technologies also have enhances the capacity of Governments, enterprises and individuals to conduct surveillance, interception and data collection*"[5].

At the heart of the Commissioner's report lies the concern that the rights held by citizens offline must also be protected online, especially in consideration of the fact that interference in the peaceful enjoyment of rights is likely to be easier, quicker, subtler and more difficult to detect and prevent online.

2. Interferences: limits, risks and protection

Traditionally, the first concern about interference in privacy comes from the exercise of public power affecting the private life of citizens and limiting its full enjoyment.

In a democratic society this may occur frequently, but State intervention should not be arbitrary or unlawful[6].

Interferences should not take place except in cases envisaged by the law, and national legislation needs to comply with certain requirements to be legitimate in an international perspective: it must be consistent with international Covenants; reasonable and necessary in the particular circumstances, and proportional to the aim sought.

[5] "*The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights*" presented at the 27th Session of the Human Rights Council on 30 June 2014.

[6] The European Convention on Human Rights, Article 8 par. 2, states that: "*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

Proportionality has become a fundamental concept, especially in recent years with measures taken to combat terrorism, and Governments adopting mass surveillance measures seeking to justify them on grounds of national security.

In her report, the Commissioner recognizes that: "[…] *digital communication technologies can be, and have been, used by individuals for criminal objectives" and that "surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a legitimate aim*".

This in itself is not sufficient: the measures of surveillance adopted by States must be proportionate as well ("*the less intrusive instrument amongst those which might achieve the desired result*"), otherwise they may be deemed to be illegitimate even if they have a legitimate purpose and have been adopted on a legal basis.

In other words, a balance should be struck between the requirements of the State and privacy safeguards.

Mention should also be made of the fact that Governments often require private enterprises to grant them direct access to the communications and personal information of their customers, and then retain this information.

Such measures may give rise to an abuse of public power[7].

In conclusion, it is clear that violations are more frequent and less easily detected, and, as a result, it is harder for citizens to obtain a remedy[8].

[7] "Mandatory third-party data retention is a recurring feature of surveillance regimes in many States, where Governments require telephone companies and Internet service providers to store metadata about all their costumers' communications and locations for subsequent access by law enforcement and intelligence agencies. This appears neither necessary nor proportionate". Extract from the Press Conference on the right to privacy in the digital age, UN High Commissioner for Human Rights.

[8] See on this point two editorials in the Oxford Journal, International Data Privacy Law, to which the Commissioner's report refers. The first editorial, entitled "Systematic government access to private-sector data" (International Data Privacy Law, 2012, Vol. 2, N. 4) provides an in-depth analysis of the multiple issues arising from the governments' constant request for access to customer data, with a final observation that: *"[…] even in the countries with the broadest and most systematic data protection law, data collection and use for national security and law enforcement are generally beyond the scope of those laws or constitute an express exception to them*".In April 2014, after the data leaks scandal, an addendum to the first editorial was published (International Data Privacy Law, 2014, Vol. 4, N. 1). See also the contributions on the subject by the non-governmental digital rights organization, European Digital Rights.

According to the UN High Commissioner: "*Effective remedies to violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms*".

3. The ruling of the Court of Justice of European Union (CJEU) on the Data Retention Directive

The Courts clearly play a leading role in providing remedies to violations of the right of privacy.

It is important to consider in this connection the recent judgment of the CJEU on joined cases C-293/12 and C-594/12[9] that casts light on digital privacy.

The Court was called upon to decide if the European Directive 2006/24, that laid down the obligation on the providers of electronic communications services to retain for a certain period of time the persona data of their costumers,[10] was compatible with the right of privacy regulated in Article 7 of the Charter of Fundamental Rights of the European Union [11] and in Article 8 of the European Convention on Human Rights; and if it was compatible with Article 8 of the Charter, concerning personal data protection.

The first point of the Court's reasoning was to ascertain whether the aims and provisions of the Directive satisfied a general interest, and the Court

[9] Judgment of the CJEU, C-293/12 and C-594/12, 8 April 2014.

[10] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available communications services or of public communications networks and amending Directive 2002/58/EC.
Article 5 listed the categories of data to be retained, including data necessary to trace and identify the source of communication (e.g., telephone number, e-mail, Internet user-ID).
Article 6 laid down the period of data retention as not less than six months and not more than two years from the date of the communication.

[11] See the Charter of the Fundamental Rights of European Union 2010/C 83/02. Article 7 (Respect for private and family life) states that: "*Everyone has the right to respect for his or her private and family life, home and communications*". Article 8 (Protection of personal data) states that: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority*".

concluded that this was the case[12].

However, it is widely recognized that the aim of "national security" is not sufficient: any interference by the public authorities must take place within certain limits, otherwise the fundamental rights of citizens would be infringed. EU legislation was necessary to lay down "*[…] precise rules for governing the scope and application of the measure*"[13] provided in the Directive; and here, the Court found more than one fault.

First, the Court underlined that the Directive does not specify a clear relationship between the data retained and a threat to public security; second, there is no provision determining a limit to the access to personal data by national authorities; and moreover, data protection safeguards are painfully lacking[14]. The conclusion of the Court is that the EU legislation under scrutiny does not comply with the principle of proportionality between its scope and its concrete measures of application: as a result the Directive is invalid.

4. Conclusion

In her report the UN Commissioner made a number of references to the judgments of European Courts, highlighting their effectiveness in identifying the matter at stake, and in providing a remedy.

However, in the collective effort to find a solution to the problem of violation of digital privacy, the Courts cannot be the sole actors.

---

[12] On this point, in paragraphs 43 and 44 of the decision the Court stated that: "*Because of the significant growth in the possibilities afforded by electronic communications, […] data relating to the use of electronic communications are particularly important and therefore valuable tool in the prevention and the fight against crime, in particular organized crime. […] It must therefore be held that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data […] genuinely satisfies an objective of general interest*".

[13] See par. 54 of the decision.

[14] After listing the above mentioned "faults" in the Directive, the Court comes to the conclusion that it "*[…] does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use*". In one of the last paragraphs of the decision, the Court also deals with matters of territoriality, stating that "[…] the Directive does not require the data in question to be retained within the European Union", which leads to evident problems of lack of control for their protection.

Greater openness between States and cooperation with private intermediaries are among the first steps to take, but, for the moment, this appears to be more of a statement of principle than an effective remedy.