Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems[*]

di Luca Pietro Vanoni **
(14 giugno 2017)

1. Introduction

A few years ago, in the movie *Captain America: Civil War*, the American government was frightened by the uncontrolled use of power by superheroes and sought to bring them under government authority, forcing them to register with an oversight body and thus give up their secret identities. This move split the superhero world in two, with one faction following the lead of Iron Man, a fervent supporter of the government's approach and the necessity to sacrifice privacy in the face of national security, and the other headed by Captain America, a dogged defender of the American dream and his right to secrecy as a person and as a superhero.

The ensuing epic duel between our two superheroes clearly tells the tale of the battle between national security and privacy our democracies are forced to confront in the age of global terrorism. This conflict reached its apex in the Datagate scandal, that is, the global surveillance disclosures that began in June 2013 with former NSA contractor Edward Snowden revealing details of secret surveillance programmes like PRISM and TEMPORA. These allowed American intelligence agencies such as the NSA and FBI (as well as GCHQ in Britain and DGSE in France) to acquire and store an unprecedented amount of digital information through cooperation with leading telephone and internet providers. These revelations inevitably sparked a debate in Europe and America on the right to privacy and personal data protection in the age of digital terrorism. A comparative analysis of these two systems can thus help in understanding the difficult balance between privacy and security in our democracies. At the end of the film, Captain America turns to Iron Man and asks him how far individual rights can be compressed in the name of national security before this ultimately damages the values of freedom and justice our constitutional democracies were created to uphold. It is a question that sums up the problem well.

2. Data Protection in European Union law: an Overview

Protection of the right to privacy and the use of personal data in Europe is especially extensive, based on Convention 108 – Council of Europe, on the legal devices of the European Union (EU) and on the case law of the European Court of Human Rights (ECHR) and the European Court of Justice (ECJ).

In the EU, the right to privacy is guaranteed and governed both by the Treaties and secondary legislation. Following the approval of the Lisbon Treaty, Article 16 of the Treaty on the Functioning of the EU governs the fundamental right to the processing of personal data, establishing the procedures for the legislative protection of this sphere. Article 16 establishes the competences of

[*] Forthcoming in L. Violini, A. Baraggia (eds.), *The Fragmented Landscape of Fundamental Rights Protection in Europe: The Role of Judicial and Non-Judicial Actors*, Elgar Publish

the EU for protecting personal data, indicating the European Parliament and the Council, acting in accordance with ordinary legislative procedure, shall approve rules able to safeguard citizens against the undue use of their personal data by EU institutions and Member States when carrying out activities which fall within the scope of Union law[1]. This article operates in conjunction with all European competences, especially internal market provisions, as the creation of this market - along with the arrival of the digital era - has resulted in the constant transmission of digital information and data. By establishing the legal basis for European data processing on recognizing a fundamental freedom, Article 16 clarifies that "where a conflict between privacy protection and the circulation of personal data makes finding a balance impossible...the former must prevail."[2]

Additionally, "constitutional" protection of the right to privacy and data protection are expressly guaranteed to every individual by Articles 7 and 8 of the EU Charter of Fundamental Rights. Article 7 specifically sets out the general provision that "Everyone has the right to respect for his or her private and family life, home and communications."[3] Article 8 safeguards "the right to the protection of personal data" establishing that 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" and that every individual "has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[4] The protection of personal data is both independent of the right guaranteed in Article 7 and a specification thereof since it regulates the protection of the individual and its nature in relation to the digital-era challenges of adopting the principles set out by the Preamble to the Charter, according to which the protection of European rights must be guaranteed "in the light of changes in society, social progress and scientific and technological developments."[5]

Special legislative acts actually guaranteed this right even before these rules were adopted in the Treaty. For many years, the main tool - albeit along with other specific acts - for such protection was the EU Data Protection Directive (95/46/EC), which required Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data."[6]

---

1 Art. 16 "1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

2 Bruno Cortese, 'Protezione dei dati di carattere personale nel diritto dell'Unione europea' [2013] in Diritto dell'Unione Europea no. 2, 316.

3 Charter of Fundamental Rights of The European Union 2012/C 326/02 art. 7.

4 Id. Art. 8.

5 See Charter of Fundamental Rights of The European Union 2012/C 326/02 at Preamble. See also Filippo Donati, 'Art. 8. Protezione dei dati di carattere personale', in Raffaele Bifulco, Marta Cartabia and Alfonso Celotto (eds) *L'Europa dei diritti* (Il Mulino, 2001) 83.

6 Art. 1 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281/31 (1995).

This act was recently replaced by what is often called the "personal data protection package", consisting of Regulation (EU) 2016/679[7], which introduces uniform, general rules in Union law, and Directive (EU) 2016/680[8], which governs data protection in relation to police and judicial cooperation when preventing, investigating, detecting or prosecuting criminal offences. These provisions now provide pervasive new privacy protection, adopting the indications issued by the European Court of Justice and Article 29 Working Party in interpreting Union law. Some of the key innovations are the right to be forgotten, the right to data portability, and the right to transparent, honest information about the processing of one's data and any breaches. Finally, the creation of the role of Data Protection Officer (DPO) is another notable change as this role is entrusted with the key tasks in checking data security and processing.

The personal data protection package is far too broad and detailed to be covered thoroughly in this work. Generally, it seeks to give the Union "an updated legislative fabric" that is "more suited to today's needs" by defining precise, robust rules that will undoubtedly have a significant influence across European law. It represents an "enormous leap forward for data protection, especially because it marks the change from a system of a directive harmonizing differing national laws based on mutual recognition to a system based on Regulation, which is, by its very nature, binding for all Union citizens."[9]

3. Data Protection and National Security between European Union and Member States

Despite this legislative framework, "the EU data protection regime contains a number of weaknesses and derogations which dilute the capacity to protect privacy rights."[10] The primary shortcoming lies with the Member States being competent for national security, which comes into conflict with the right to privacy when sophisticated digital data collection and storage programmes are used.

The EU has tried on occasion in the past to adopt legislative measures to harmonize national laws on foreign politics and common defence[11], but national security remains the responsibility of Member States. As set out in Article 4(2) EU Treaty, "The Union shall respect the equality of Member States before the Treaties as well as their national identities…. It shall respect their essential

7 Regulation (EU) 2016/679 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), O.J. L 119/1 (2016).

8Directive (EU) 2016/680 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, O.J. L 119/89 (2016).

9 Francesco Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, (Giappichelli, 2016), 177.

10 David Cole and Federico Fabbrini, 'Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders', [2016] *14 I•CON*, 255.

11 Valsamis Mitsilegas et Al., *The European Union and Internal Security* (Palgrave Macmillan, 2003).

State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."[12] This recognition of exclusive State competence has practical implications right down to secondary legislation level. For example, the EU Data Protection Directive (95/46/EC) allows Member States to adopt legislative measures to restrict the scope of the obligations and rights provided "when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security…"[13], and these exceptions were recalled by the recent Regulation (EU) 2016/679[14].

Specific legislation also has provisions establishing exceptions to the digital privacy of citizens. For example, in 2006 the European Parliament approved the Data Retention Directive (2006/24/EC)[15], which allows Member States to store telephone and computer metadata for public security purposes and for preventing crime and terrorism. This provision has now been invalidated by the Court of Justice, but it was adopted following the London underground bombings in 2005. It was an attempt to define the European balance between individual rights to data protection and the intelligence needs of States. The clash between these two rights is an issue for all western democracies, but in Europe it is an example of the "special European federalism"[16] and the EU's constitutionalization process initiated with the Treaty of Lisbon.

This conflict, while remaining part of the division of competences between Union and Member States, will become ever more accentuated because of the numerous State laws approved by countries in response to the ever-increasing number of terror attacks in our societies. The United Kingdom, France, Germany and most recently Italy have established digital surveillance programmes to thwart the terrorist threat before attacks actually occur.[17] These

12 Art. 4 (2) Treaty of European Union, O.J. C 326/1 (2006).

13 Data Protection Directive, *supra* note 6, art. 13

14 Regulation (EU) 2016/679, *supra* note 7, art. 16 Considering: "This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union." See also art. 23: "Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: a) national security; b) defence; c) public security ..."

15 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. L 105/54 (2006).

16 Giovanni Bognetti, 'Lo speciale federalismo europeo' Angelo Maria Petroni (eds*) Modelli giuridici ed economici per la Costituzione europea* (Il Mulino, 2001) 245.

17 For a recent comparative analysis of the legislative measures concerning terrorism, see Laurent Mayali and John Yoo, 'A Comparative Examination of Counter-Terrorism Law and Policy' [2016], UC Berkeley Public Law Research Paper No. 2949078, Available at SSRN: https://ssrn.com/abstract=2949078. For Italy see Giovanna De Minico, 'Le libertà fondamentali in tempo di ordinario terrorismo', [2015] Federalismi.it no. 10/2015, http://www.federalismi.it/nv14/articolo-documento.cfm?Artid=29517.

measures use technologies that require digital databases and hence the collection of electronic data from citizens. The 'laws of fear' in question fall under State responsibility and are not directly subject to Articles 7 and 8 of the Charter, as clarified by Article 51, since these "are addressed to the institutions, bodies, offices and agencies of the Union", while the Member States are merely required to respect them "only when they are implementing Union law." As a result of how competences are assigned, protecting the privacy and ensuring the security of citizens is really entrusted to national, not European, legislation.

Nonetheless, the integration between European and national law is such the rights in the Charter do influence political and legislative decisions, and often do so quite substantially. This is even more true because of the interpretation of Treaties by the Court of Justice, which "has long extended the scope of application of the fundamental rights it interprets...identifying the implications in Member States and binding even national bodies and institutions."[18] Thus, decisions by judges in Luxembourg provide an essential perspective in understanding the actual sphere and scope of European privacy law where State or European laws come into conflict with the provisions in Articles 7 and 8 of the Charter.

4. Digital Privacy before the Court of Justice of European Union

Court of Justice rulings on digital privacy provide an especially important approach to defining the sphere and scope of this right. The Court was initially exceptionally wary in its case rulings, but it now seems to have carved out a role as a protagonist even when it comes to concretely defining the rights established by Articles 7 and 8 of the Charter.

This change in approach by EU judges can be traced particularly to 2014 and the following cases: C-131/12 *Google Spain* (2014)[19], C-293/12 and C-594/12 *Digital Rights Ireland* (2014)[20], C-362/14 *Schrems* (2015)[21] and finally C-203/15 and C-698/15 *Tele2 Sverige and Watson* (2016)[22]. These four rulings are a fundamental starting point for understanding the extent and scope of Articles 7 and 8 of the Charter and for finding the balance that judges have adopted between those rights and conflicting interests/rights. The *Digital Rights Ireland* and *Schrems* cases sought to balance digital privacy and security; the *Google Spain* case attempted to resolve the conflict with another freedom - the freedom of expression - in the digital world. However, the latter case is as important as the other two in understanding the reasoning of European judges in relation to the protection of privacy in Europe.

---

18 Marta Cartabia, 'Art. 51. Ambito di applicazione', in Raffaele Bifulco, Marta Cartabia and Alfonso Celotto (eds.) *L'Europa dei diritti* (Il Mulino, 2001) 347.

19 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317

20 Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger and others*, ECLI:EU:C:2014:238.

21 C-362/14 *Maximillian Schrems c. Data Protection Commissioner*, ECLI:EU:C:2015:650.

22 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB (C203/15) v. Postoch telestyrelsen, and Secretary of State for the Home Department (C698/15) v. Tom Watson and Others,* ECLI:EU:C:2016:970.

In the *Google Spain* case, the Court of Justice was petitioned in relation to a request for Google to remove links from search results to web pages that were potentially harmfully or were no longer relevant to the person. The claimants thus sought a true right to be forgotten in relation to web data, arguing that Google's web page indexing amounted to the collection of personal data. The Court's incredibly broad (some have even called it "manipulative"[23]) interpretation of the rules in the Directive accepted the claimants' arguments and ruled they were entitled to have links to web pages containing personal data removed from search results, without any changes to the actual web pages and without the publication of such information being in any way illegal.

This interpretation is the result of the "constitutionalization" of the privacy set out in the Charter. European judges thus hold that the rights granted by Articles 7 and 8 "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name" (para. 97). The Court then limited the scope of this statement by adding the recognition of this right must be weighed against the interests in play and thus requires a case by case assessment. Generally, the judges' ruling does extend the scope of the European right to privacy, as it becomes a positive right to control information about oneself (that is the "*habeas data* right"[24]).

A few months prior to the *Google Spain* ruling, the Court had almost suggested it would interpret privacy rights so broadly when it annulled the Data Retention Directive in the *Digital Rights Ireland* case. As noted, this directive was introduced to harmonize national legislations governing the mass storage of metadata from digital traffic to prevent serious crimes. The directive set out that such data could be stored for no less than six months and no more than two years. In deciding the case, the Court initially noted the interference of these provisions in the rights established by Articles 7 and 8 of the Charter was "particularly serious" because it is "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance" (para 37).

Based on these considerations, the judges assessed whether the interference was justified - in the light of Article 52 of the Charter, which allows limitations on European freedoms provided the essence of those freedoms is respected -, met the objectives of general interests and was proportional to the purpose. In relation to the first aspect, the judges argued it did not harm the essence of this right as it was limited to the use of data and did not regard the content of the communications. Moreover, such data collection was meant to prevent and combat crime, and was consequently justified, according to the Court, for reasons of public security. However, it did fall short on the issue of proportionality for two reasons. First, the directive rules would seem to be generic and contain gaps when it comes to the people influenced by the data collection, which encompasses "the entire European population" (para 56) and

23 Oreste Pollicino, 'Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale', [2014] in Federalismi.it no. 3/2014 [no. 3/2014], http://www.federalismi.it/nv14/articolo-documento.cfm?artid=28017, 14.

24 Tommaso Frosini, 'Google e il diritto all'oblio preso sul serio', in Giorgio Resta and Vito Zeno-Zencovich (eds.) *Il diritto all'oblio su internet dopo il caso Google v. Spain*, (TrE-PRESS 2015) 2.

"covers, in a generalized manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime" (para. 57). Secondly, the directive "fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference" (para 60). The judgement's effect primarily concerns Union law and thus does not invalidated national rules. Nonetheless, the ruling does open the way for European citizens to seek the repeal of national rules on data retention by their own Courts as they breach the right to the protection of personal data[25]. Unsurprisingly, in the wake of the Court of Justice ruling, many national legal systems effectively declared the rules unconstitutional and thus highlighted the increased importance of this right across the continent[26].

The cases analysed have marked the first increase in the level of privacy protection in the EU. Various reasons underlie such conduct, including the reasonable hypothesis of the tension between European countries and the United States that grew out of Snowden's revelations about the NSA's operations. This tension reached its apex with the *Schrems* ruling, in which the Court invalidated the Safe Harbour agreement between the European Commission and the United States on data transmission between the two sides of the Atlantic. The case was brought by an Austrian lawyer, Maximillian Schrems, who initially petitioned the Irish authorities and then the Court of Justice seeking to have the transfer of his personal data acquired via Facebook from the Irish subsidiary of that company to its Californian parent declared illegitimate. The cross-border traffic of digital data has long been a fundamental tool in trade relations between Europe and America. In order to implement Directive 95/46/EC, the European Commission had adopted Decision 2000/520/EC authorizing the transfer of data from the EU to US companies that had ratified the Safe Harbour principles (i.e. adopting the principles of privacy protection set out in European law)[27].

In *Schrems*, the Court invalidated that decision, arguing it "cannot prevent persons whose personal data has been or could be transferred to a third country from lodging with the national supervisory authorities a claim … concerning the protection of their rights and freedoms in regard to the

25 See Federico Fabbrini, 'The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.', [2015] *28 Harv. Hum. Rts. J.* 88: "the ECJ decision does not automatically remove national implementing acts from the legal order .... However, because national data retention laws are technically exceptions to the Data Protection Directive, they are subject to review for compatibility with EU human rights law."

26 See Niklas Vainio, Samuli Miettinen, 'Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States', [2015] *Int J Law Info Tech* 23 (3), 290.

27 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

processing of that data." (para 53). This strengthened the powers of national authorities, which had to be able to independently assess if the transfer of a person's data to a country outside the Union complied with the directive. Secondly, the judges focused on the Commission decision, determining whether this met European data protection standards. On this front, the judges noted the Safe Harbour regime is binding for American companies that sign it, but is subordinate to requests by the US government when such requests are justified on national security grounds. In essence, the American Safe Harbour system does not genuinely protect the privacy of European citizens because it does not prevent such data from being accessed by American agencies in accordance with current US law. Consequently, the Court ruled the Commission's decision to be invalid as a rule "permitting the public authorities to have access on a generalized basis to the content of electronic communications" compromises "the essence of the fundamental right to respect for private life" (para 94) when (as in the current case) it does not provide for "any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data" (para 95).

The last chapter in the ECJ privacy saga is the *Tele2 Sverige and Watson* case. In that ruling, the Grand Chamber further strengthened the privacy protection afforded to European citizens, holding that national laws that establish a general and indiscriminate obligation on electronic communication service providers to store client data and that allow national authorities generalized access to such data were incompatible with Union law. The matter had been brought before the Court by two national courts (Kammarrätten i Stockholm and Court of Appeal England & Wales) and specifically concerned the interpretation of Article 15 of the Electronic Communications Directive (2002/58/EC), which allows Member States to require public electronic communications service providers to retain data about communication activities for certain defined public interests such as the fight against terrorism and serious crime.[28]

The Court provided a restrictive interpretation of Article 15, establishing that it "must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication" (para 112). The storage of such data is only permitted when national legislation "indicates in what circumstances and

28 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, O.J. L 201 (2002) art. 15: "1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

under which conditions a data retention measure may, as a preventive measure, be adopted, thereby ensuring that such a measure is limited to what is strictly necessary" (para 109). Consequently, the Court "challenges the compatibility of mass data retention with Articles 7 and 8 EUCFR even in the context of the fight against terrorism,"[29] establishing that exceptions to the right to data protection should be limited to what is absolutely necessary. This interpretation also extends to the requirements for national authorities to access such data. As the *Tele2 Sverige* ruling noted, EU law "must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union" (para 125).

Starting from the *Google Spain* case, the Court of Justice would seem to have taken on a leading role in defining the right to digital privacy in Europe. Following this ruling, the cases heard by EU judges have resulted in a significant strengthening of that freedom in "constitutional terms", establishing the primacy of this right over other, also legitimate rights and interests. The level of protection of digital data is thus higher than in the rest of the world, especially than in America. Concerning the question of national security, the Court's reasoning would seem to move in concentric circles that progressively restrict this public interest. Following the *Tele2 Sverige* ruling, the "obligation to 'take digital data protection seriously' falls not only to European (*Digital Rights Ireland*) and American (*Schrems*) institutions, but also binds Member State legislators."[30] In essence, the Court has adopted an almost political stance, affirming the "digital sovereignty" of the European Union over data processing and "establishing its [own] judicial supremacy over questions of the highest political level."[31] Yet, at the same time the "data-centric" approach of the European Union creates a potential risk of radicalizing the right to privacy to the detriment of legitimate interests and rights that are also "constitutionally" protected, thus marginalizing, for example, the requirements of freedom of online information or national security measures.

5. Privacy in the United States of America: Constitutional Framework

In the United States of America, safeguarding confidentiality has been a fundamental value since the very birth of the Federation. Even before Warren

29 See Lorna Woods, 'Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)' (eulawanalysis 21 December 2016) http://eulawanalysis.blogspot.it/2016/12/data-retention-and-national-law-ecj.html access 20 April 2017.

30 Oreste Pollicino and Marco Bassini, 'La Corte di giustizia e una trama ormai nota: la sentenza *Tele2 Sverige* sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico' [2017] DPC http://www.penalecontemporaneo.it/d/5162-la-corte-di-giustizia-e-una-trama-ormai-nota-la-sentenza-tele2-sverige-sulla-conservazione-dei-dati, access 28 April 2017.

31 Vincenzo Zeno-Zencovich, 'Intorno alla decisione nel caso Schrems: la sovranità digitale e il Governo internazionale delle reti di telecomunicazione', in Giorgio Resta and Vito Zeno-Zencovich *La protezione transnazionale dei dati personali*, (TrE-PRESS 2016) 9.

and Brandeis famously defined the "right to be alone"[32], the fathers of the American Constitution placed enormous importance on the freedom of the individual because, during colonial times, they hated the arrogance with which English officials would search their property and communications without any form of judicial review[33]. Once the English had been defeated, this widespread mistrust of excessive governmental control was codified in the Fourth Amendment to the American Constitution, which establishes the right of citizens "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[34] This article is still the standard on which the American right to privacy is based, as well as being one of the pillars of the system of criminal law and procedures. Nonetheless, the modern meaning and role of that clause has changed in at least two ways.

First, technological development has strongly influenced its implementation because the American Framers could never have imagined the extent of the impact of the digital revolution on people's lives and this has necessitated a series of interpretative adjustments by judges and legislators. By the early 20th century, the Supreme Court had already had to reconsider the meaning of the constitutional amendment for phone tapping, that is, to interpret the clause for a technology not envisaged by the American constitution. In society today, this problem has grown substantially as widespread use of technology constantly generates new interpretation problems.

Secondly, the fight against terrorism influences the right to privacy because the arrival of the digital era has provided everyone - including terrorists - with new communication means that make it easier to recruit potential terrorists and plan attacks. To protect national security, the American government has devised mass digital data collection programmes that try to obtain, before an attack, information that can be used to prevent attacks before they happen. Clearly, this requires a pre-emptive, widespread investigative approach that could easily invade the privacy of individuals. Consequently, American legal scholarship has begun to debate the role of the Fourth Amendment in the age of the global digital war since, as can easily be realized, "the current criminal laws and traditional enforcement process cannot provide absolute protection against terrorist acts" and "traditional Fourth Amendment requirements may thwart many investigations of terrorism, which depend on stealth to prevent terrorist plans before they are carried out."[35]

Bearing in mind these two considerations, it is now necessary to look at how privacy, as regulated under the Constitution, differs in America and Europe. First, a distinction has been made since *United States v. United States District Court (1972)*[36] between personal privacy in relation to ordinary criminal acts and those that have an influence on national security. The latter are considered to fall under the constitutional provision that the President has to "preserve, protect

32 Samuel Warren and Louise Brandeis, 'The Right to Privacy', [1890] *4 Har. L.R.* 193.

33 William J. Cuddhy, *The Fourth Amendment: Origins and Original Meaning*, (Oxford University Press 2008).

34 U.S. Const. Am. IV.

35 William C. Banks and Marion E. Bowman, 'Executive Authority for National Security Surveillance', [2000] *1 Am. U. L. Rev 50*, 92.

36 *United States v. U.S. District Court*, 407 U.S. 297 (1972)

and defend the Constitution of the United States."[37] A further distinction is made between internal threats, which are covered by the safeguards envisaged in the Fourth Amendment, and external ones, which are tied to the actions of foreign States or agents. The protections afforded in the latter case are significantly weakened to bolster national defence.[38]

Secondly, while Articles 7 and 8 of the European Charter recognize the right to digital privacy for "everyone", the American Constitution differentiates between citizens and foreigners. On American soil, the application of the Fourth Amendment is guaranteed for both Americans and foreigners, but this same level of protection does not apply to government surveillance outside of the Federal borders. The Supreme Court ruling in *United States v. Verdugo-Urquidez (1990)*[39] reiterates this Amendment can only be applied to limit government surveillance if it "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection" with this community.

Finally, the Supreme Court's interpretation of the Fourth Amendment has created a series of doctrines that would seem to restrict the sphere to which privacy applies. The original wording of the Amendment refers primarily to the protection of the physical limits of citizens' privacy, defining these against illegitimate searches of "persons, houses, papers, and effects." In line with this interpretation, the Supreme Court initially applied this clause on the basis of the physical trespass doctrine, that is, against cases of police search and seizure in one of the "places" listed in the Constitution. The application of this theory led the Supreme Court, for example, to rule it was legitimate for the FBI to conduct an investigation using wiretapped private telephone conversations without judicial approval because these were obtained outside of the claimant's home (*Olmstead v. United States* 1928)[40].

As technology has spread, the Court has moved beyond that doctrine, arguing the Fourth Amendment "protects people, not places." In *Katz v. United States* (1967)[41], the Supreme Court extended and "dematerialized" the physical boundaries established by the Constitution, using the perception citizens have of their privacy to define privacy. As noted by Judge Harlan, the Fourth Amendment should protect "an actual (subjective) expectation of privacy" that society "is prepared to recognize as 'reasonable'" (p. 389). The Court's intent was the adoption of the reasonable expectation of privacy test should extend the scope of application of constitutional guarantees to cases not specifically envisaged by the Constitution, introducing - through the reasonableness principle - less rigid use of the parameters in the Fourth Amendment. This has not, though, always been the case and subsequent rulings ended up reducing the scope of constitutional guarantees.

37 U.S. Const. Art. II sec. 2.

38 Ioanna Tourkochoriti, 'The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation: In Search For Legal Protection Against Surveillance' [2014] *36U. Pa. J. Int'l L.* 459 ss.

39 *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

40 *Olmstead v. United States*, 277 U.S. 438 (1928).

41 *Katz v. United States*, 389 U.S. 347 (1967).

Starting from the reasonable expectation of privacy doctrine, the Supreme Court created a legal presumption that excludes information citizens freely reveal to third parties from the scope of the Fourth Amendment. In *United States v. Miller* (1976)[42] and *Smith v. Maryland* (1979)[43], the Supreme Court formed the third party doctrine according to which "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[44] Therefore, citizens who freely grant personal data to public service providers such as banks (*Miller*) or telephone companies *(Smith)* implicitly forgo privacy guarantees. Consequently, if government agencies acquire such information, it is not necessary to have judicial approval or probable cause. The *Smith* case is especially notable as the Supreme Court took a major step in limiting American citizens' right to privacy because applying the third party doctrine to information collected using a pen register (i.e. an electronic device that records all numbers called) installed without judicial approval on a telephone line as part of an investigation created the legal basis for extending that theory to the use and processing of computer data in the digital era.

6. Right to Privacy within the National Security Programmes

The constitutional system described above is directly acknowledged by legislation. Congress has been especially active in passing bills to govern the right to privacy. In addition to the key Privacy Act of 1974[45], the American legislative branch has approved specific laws on the protection of this right in the digital age, such as the *Electronic Communications Privacy Act* (1986)[46] and the *Communications Assistance for Law Enforcement Act* (1994)[47]. These laws definitely extend and specify the nature of this right, but they are also influenced by the constitutional limitations discussed above, for example distinguishing between the protections afforded to "US persons" and those - far weaker - that foreigners are guaranteed.[48] Moreover, the third party doctrine limits the scope of these provisions when personal data is voluntarily given to third parties, thus giving the Government legitimate national security grounds to acquire the data and metadata stored by telephone companies and internet service providers.

Privacy rules in America also conflict with specific legislative acts designed to regulate digital surveillance by the American government. For many years, national security was not the subject of specific legislative provisions as it was largely understood to be synonymous with the public order guaranteed, locally, by the police force in each State. The need to have a federal investigation service (the FBI) only became apparent as organized crime took

42 *United States v. Miller* (1976) 425 US 435.

43 *Smith v. Maryland* (1979) 442 US 735.

44 *United States v. Miller*, supra at note 43, 442-443.

45 Privacy Act of 1974, 5 U.S.C. § 552a (1974).

46 Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22 (1986).

47 Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001-10 (1994)

48 Francesca Bignami, 'The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens', [2015] Study for the LIBE Committee, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2705618.

root during probation. The end of the two World Wars and the advent of the Cold War led to the United States strengthening its intelligence system with the creation of two agencies tasked with permanently defending national security through spying (CIA) and the collection and decryption of secret messages (NSA).

For a number of years, the supervision of these agencies was largely left to the Government, but the exceptionally rapid development of surveillance techniques and the scandals linked to J. Edgar Hoover's dossiers and then Watergate forced Congress to approve legislation to limit excessive surveillance power. This led to the approval of the *Foreign Intelligence Surveillance Act* (FISA) in 1978[49], which sets out the limits of Government power in relation to privacy.

The law establishes a series of measures designed to limit the NSA's collection of sensitive data, for example, by restricting the concept of "foreign power or agent thereof" and establishing that the Government must show "probable cause" to believe the person under surveillance is a genuine security threat. Consequently, Congress has instituted special courts and review courts (*Foreign Intelligence Surveillance Court* – FISC; *Foreign Intelligence Surveillance Court of Review* – FISCR) to determine the reasonableness and legitimacy of government surveillance requests. The powers of control of these judges are far more limited than ordinary judges, consisting merely of a formal assessment of compliance with legal requirements.[50]

Numerous specific laws and regulations have followed this first one. Undoubtedly, the most important of these is the *PATRIOT Act* (2001)[51] adopted by Congress in the aftermath of the Twin Towers attacks. This law profoundly changed the organization and functioning of the US system to fight terror, heavily cutting into the privacy of citizens. Notably, the law amended various FISA rules to increase federal agency powers to collect "tangible things" that might be useful in investigations (Section 215) and to limit privacy protection to American citizens (Section 702). These measures gave NSA agents the power to obtain telephone and computer records from the main industry providers to produce a massive searchable database that could be used in investigations.[52]

Computer metadata collection programmes ran largely uninterrupted from 2006 onwards. These included the Bulk Metadata Surveillance Program, which was started by Bush and extended by Obama on more than one occasion. This requires the main telephone companies to provide the NSA with records - i.e. metadata - containing the place, time and duration of telephone calls, but not their content.[53] This metadata feeds a searchable database that could be mined to find contact between terror cells. NSA analysts have the

49 *Foreign Intelligence Surveillance Act* of 1978 (FISA), 50 U.S.C. § 36 (1978)

50 Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, (Yale Un. Press, 2011) 74-75.

51 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001(USA PATRIOT Act), Public Law 107-56 (2001)

52 Laura K. Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations', [2014] *37 Harv. J.L. & Pub. Pol'y* 2014, 757 ss.

53 ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (Aug. 9, 2013), https://perma.cc/V7VM-5MAU access 29 April 2017.

ability to use this database using an "identifier" - that is, the "contact" assumed to be involved in criminal activity - that forms the starting point or "seed" for the search (also called the "seed identifier"). Once authorized, computer analysts can process the data to find first, second and third level contacts of the seed identifier (called "three hops"). This allows the NSA to gather an almost unimaginable amount of data and indefinitely extend its search to users that - in by far the majority of cases - have absolutely nothing to do with the "reasonable articulate suspicion" that forms the standard for investigating potential terrorists.[54]

7. Digital Surveillance Programmes and Federal Judges

The Snowden disclosures also caused an uproar in the United States, with plenty of doubt about the constitutionality of this digital surveillance programme. It also produced conflicts that had to be resolved, for example, by the Federal Courts in the Columbia and New York districts. In both cases, the claimants argued the government programme was illegitimate and sought the NSA be required to suspend the bulk collection of their data (i.e. their phone and internet records) and to destroy the data already collected. While both claims largely mirrored each other, they were ruled on differently. In *Klayman v. Obama*[55], Justice R. Leon ordered the NSA to stop the programme, but in *ACLU v. Clapper*[56], Justice W.J. Pauley decided it was constitutionally legitimate. These two interpretations clearly show the tension between the need to protect citizens' freedom and their security.

In *Klayman v. Obama* (2013), the District Court for the District of Columbia ruled the indiscriminate and arbitrary collection of telephony metadata by the NSA amounted to an illegitimate search and seizure under the Fourth Amendment. To reach this conclusion, Justice Leon had to move away from the third party doctrine, stating this was conceived at a time in history when the use of mobile phones "was, at best, the stuff of science fiction" (p. 52), and it was unable to adequately protect the privacy of citizens in a cell phone-centric culture[57]. If "the basic purpose of [the Fourth] Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials" (p. 63), there is no doubt that "this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analysing it … infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment" (p. 64). This would seem to return to an interpretation of the

54 Elizabeth Atkins, 'Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment' [2014] *10 Wash. J.L. Tech. & Arts.* 87: "The metadata information the Government is able to collect, store, and search on a massive scale makes Section 215 a violation of the Fourth Amendment. The Fourth Amendment is clear: to search a constitutionally protected area, one must have probable cause and obtain a warrant from a detached and neutral judge. That is not being done under the metadata program."

55 *Klayman v. Obama*, No. 13-0881, 2013 WL 6598728, 18 (D.D.C. December 16, 2013)

56 *ACLU v. Clapper*, 959 F. Supp. 2d 724, 748 (S.D.N.Y. 2013).

57 As recalled by Justice Leon in *Klayman v. Obama*, "records that once would have revealed few scattered tiles of information about a person, now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life" (p. 54).

Constitution that uses the historical ban on government intrusion in the personal sphere of citizens, but reinterpreted in the light of current technology. In such an understanding, the traditional criterion of physical trespass should also be understood as digital trespass.

The conclusion reached but a few weeks later by the District Court for the Southern District of New York in *ACLU v. Clapper* (2014) was quite the opposite, rejecting the petition filed by the ACLU and holding the Bulk Metadata Surveillance Program was perfectly legitimate. The different conclusion was evident right from the beginning of the ruling. It focused on the tragic consequences of the 9/11 attack and noted more efficient use of computerized systems by federal agencies could have potentially prevented the attack as "telephony metadata would have furnished the missing information and might have permitted the NSA to notify the FBI of the fact that Al Mihdhar [one of the 9/11 terrorists] was calling the Yemeni safe house from and inside the United States" (p. 2). The entire judgement is thus based on national security. The NSA programme is seen as a legitimate tool to combat the terror threat in compliance with the *PATRIOT Act* and the Supreme Court's interpretation of the Fourth Amendment.[58] For this aspect, Justice Pauley drew from *Smith v. Maryland* the constitutional parameters for deciding on the case. Citizens are aware telephone companies store metadata for commercial reasons and hence - applying the third party doctrine - they cannot have a reasonable expectation for the privacy of such information "because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment" (p. 44).

This decision was vacated on appeal for procedural reasons linked to the legal foundation for the Bulk Metadata Program (*ACLU v. Clapper II*[59]). Yet, exploring the argument made in Justice Pauley's decision, it would seem to return to the problem of the relationship between privacy and security based on the third party doctrine. It is noted in the ruling people voluntarily provide personal data to multinationals that use this for commercial purposes, but even though such information is far more relevant and invasive than telephony metadata, only a few people seem worried by it.

8. Conclusions

Analysing privacy and personal data protection in Europe and America shows differing legal and political approaches. Particularly following the adoption of the Charter of Fundamental Rights of the European Union, the EU would appear to guarantee an exceptionally high degree of privacy protection. This is reinforced by the interpretation in Court of Justice rulings in recent years, such that Europe can today be seen as "the fortress of digital privacy."

By contrast, in the United States privacy protection has weakened as the technology used in combating international terrorism has improved. The legislative and constitutional tools safeguarding this right would seem to be inadequate in the face of the challenges of the digital era. For example, the third

58 See *ACLU v. Clapper* p. 36: "Congress was clearly aware of the need for breadth and provided the Government with the tools to interdict terrorist threats."

59 *ACLU v. Clapper*, No. 14-42-CV, 2015 WL 2097814, (2d Cir. 2015).

party doctrine has long been criticized in legal scholarship[60] and recently various Supreme Court Justices (Alito; Sotomayor) have seemed to be prepared to move beyond that doctrine in their concurring opinion in *United States v. Jones* (2012)[61].

The two systems clearly differ in approach, but comparing them also brings to the surface various points that could be useful in defining a common, global approach to privacy.

First, America is slowly changing its position on personal data protection. In the wake of the debate sparked off by Datagate, the President and Congress approved the *Judicial Redress Act* (2015), which (partially) extended privacy protection to non-American citizens, and the *FREEDOM Act* (2015)[62], which curtailed the American government's surveillance powers. These hesitant first steps towards broader protections for citizens should be viewed positively, although they are unlikely to provide definitive solutions.

Secondly, the America system might have some shortcomings, but the approach adopted does question the European balance between privacy and other interests/rights that (especially in Court of Justice rulings) seem to have been forgotten. On the national security front, the lack of interest at European level is largely because such an interest falls under Member State competence and so does not directly relate to Union law. In the United States, by contrast, the correct balance between privacy and national security is a true challenge faced entirely by the federal government. As the 2013 Intelligence Report commissioned by President Obama noted, "the problem here is that the United States Government must protect, at once, two different forms of security: *national* security and *personal* security (which is "the right of the people *to be secure* in their persons, houses, papers" established by the Fourth Amendment.)"[63] Europe does not have to deal with the same problem. As European citizens, we want the Union to provide a high level of protection for our personal data and, at the same time, we look to our State governments to protect us from terrorist attacks. This asymmetry makes it far easier for the EU to guarantee substantial privacy protection, but it does not fully resolve the balance between privacy and the security of individuals.

Finally, business and trade, along with the multidimensional nature of the digital era make it necessary to have an agreement between the two legal systems about privacy protection on both sides of the Atlantic.[64]The Privacy

60 See, among others, Laura K. Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations', supra note 53; Ioanna Tourkochoriti, 'The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation: In Search For Legal Protection Against Surveillance', supra note 38.

61 *United States v. Jones*, 565 US _ (2012) concurring opinions Justices Samuel Alito and Sonia Sotomayor.

62 Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA FREEDOM Act) Pub.L. 114-23 (2015).

63 See Liberty and Security in a Changing World - Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies 14-15 (12 December 2013) https://www.nsa.gov/about/civil-liberties/resources/assets/files/liberty_security_prgfinalreport.pdf access 27 April 2017.

64 David Cole and Federico Fabbrini, *Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders*, supra note 4, 236.

Shield agreement is an example of this. It replaces the earlier Safe Harbour system the Court of Justice found to be illegitimate. In terms of the national security question, mention must be made of EU Directive 2016/681 (2016)[65] on the use of passenger name records (PNR) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. The problem of data monitoring on both side of the ocean cannot be resolved simply by defining high levels of privacy protection in each system. It requires joint efforts to find areas of agreement that correctly balance the various interests/rights in play. On this issue, special attention must paid to the actual use of government digital surveillance programmes given the purposes of such programmes. As a New American Foundation investigation found, the NSA's collection of metadata was not always proportional to the goal nor was it especially useful in uncovering terrorist plots.[66] At the same time, metadata collection programmes originated to resolve communication problems between federal agencies highlighted by the 9/11 Commission. They are a fundamental tool for preventing terrorist attacks because, as the then NSA Director Keith Alexander said, "there is no other way we know of to connect the dots."[67]

It is no simple task to determine precisely which of the two judgements better fits reality. Yet, that merely makes it more important and pressing to find the right balance between security and privacy. As Benjamin Franklin noted at the birth of the American Constitution, "they who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

** Ricercatore di Diritto Costituzionale – Università degli Studi di Milano

65 Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, O.J. L 119/132 (2016).

66 See Peter Bergen, David Sterman, Emily Schneider and Bailey Cahall, 'Do NSA's Bulk Surveillance Programs Stop Terrorism?' *New American Foundation Report* (14 January 2014) http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists access 29 April 2017: "However, our review of the government's claims about the role that NSA "bulk" surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading. An in-depth analysis of 225 individuals recruited by al-Qaeda or a like-minded group or inspired by al-Qaeda's ideology, and charged in the United States with an act of terrorism since 9/11, demonstrates that traditional investigative methods, such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance programs to these cases was minimal. Indeed, the controversial bulk collection of American telephone metadata, ... appears to have played an identifiable role in initiating, at most, 1.8 per cent of these cases."

67 See Spencer Ackerman, 'NSA chief on spying programs: "There is no other way to connect the dots", *The Guardian–on line* (Washington 13 December 2013) https://www.theguardian.com/world/2013/dec/11/nsa-chiefs-keith-alexander-senate-surveillance access 2 May 2017.