The Right to Privacy and New Technologies: Between Evolution and Decay*

Fabrizio Petrucco

Abstract

The purpose of this study is to briefly analyze the right to privacy historical origins and latest evolutions, from its first, yet frail, appearance in XVIII century Europe to the recent Regulation (EU) 2016/679 implementation.
The first part of the essay addresses privacy's emergence as an autonomous right. A long-running process, during which it will go from being associated to more prominent rights, as the right to property (in the UK) or to dignity (in France), to finally find its scientific emancipation in the world-famous Warren and Brandeis' article "The right to Privacy".
The second part, instead, focuses on the inclusion by the United States and EU legal orders of *data privacy*, a new form of privacy trying to cope with the still ongoing digital revolution. In particular, the study will try to highlight how privacy's different notions on the two side of the Atlantic, have been reflected by both its means of protection and case-law.
Once established the EU lead in privacy's promotion, the third part of the essay will tackle the current challenges to its protection, specifically the personal data monetization and antiterrorism politics.

Summary

Keywords

Privacy, Data protection, Technologies, Personal data, Data privacy

*L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio a "doppio cieco".

1. Introduction to the origins of privacy

Norberto Bobbio stated that fundamental rights are an historical product, gradually generated by the fight for new freedoms against the old powers[1]. According to his theory, human rights dimension is inevitably marked by historical, political, social, economic and technological factors. This relationship forces fundamental rights to continuously re-shape their content and boundaries on one hand, yet it enables them to cope with our ever-changing reality on the other[2]. However, as new rights arise from the society, they do not overrule the previous ones, as the universe of rights lives on accumulation rather than replacement[3]. This very dynamic, allowed scholars to recognise different generations of fundamental rights[4], raising, at the same time, concerns about an "inflation" of human rights resulting in their loss of value[5].
The first generation consists in civil and political rights, which emerged during the liberal revolutions imposing severe restraints on the State, thus been called "negative" freedoms[6]. Afterwards, in XIX and XX centuries, a second generation arose from the working class struggles for social justice and widened participation. Scholars refer to this new set of freedoms as "positive", as they require the State to actively remove the social barriers which prevent the deprived sectors of society from enjoying basic rights as healthcare, education and to extend the right to vote (empowerment of the masses)[7]. Finally, the social and scientific revolution led Constitutionalism to recognise two more generations of rights[8]. However, the technological revolution speed is deeply questioning the Law capability to cope with such an astonishing fast pace. Indeed, the new technologies started very soon to threaten - under many aspects - old and new

---

1 N. Bobbio, *L'Età dei diritti*, Torino, 1992, XII-XIII.

2 G. Zagrebelsky, *Il diritto mite*, Torino, 1992, 105, 107-108; J. Galtung, *I diritti umani in un'altra chiave*, Milano, 1997, 202-206; P. Ridola, *Diritti fondamentali. Un'introduzione*, Torino, 2006, 22.

3 E. Brugiotti, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Dirittifondamentali.it*, 2, 2013, 1; R. Kreide, *Politica globale e diritti umani, Potenza e impotenza di uno strumento politico*, Torino, 2010, 38; N. Bobbio, *op. cit.*, XVI.

4 A. Spadaro, *Dai diritti individuali ai doveri collettivi. La giustizia distributiva nell'età della globalizzazione*, Soveria Mannelli, 28 ss.; R. Bin-G. Pitruzzella, *Diritto costituzionale*, Torino, 2015; A. Barbera-C. Fusaro, *Corso di diritto costituzionale*, Bologna, 2016; C. Tomuschat, *Human Rights: Between Idealism and Realism*, Oxford, 2008, 25 ss.; L. Mezzetti, *Manuale breve. Diritto costituzionale*, Milano, 2013, 501 ss.

5 M. Cartabia, *L'universalità dei diritti umani*, in *Quaderni costituzionali*, 3, 2009, 560; *contra* S. Rodotà*, L'età dei diritti. Le nuove sfide*, in Aa. Vv., *Lezioni Bobbio*, Torino, 2006, 60-61.

6 R.R. Palmer, *The Age of Democratic Revolutions*, Princeton, 1959; G. Gusford, *Les révolutions de France et Amérique*, Paris, 1988; G. Bognetti, *Lo spirito del costituzionalismo americano*, Torino 1998; B. Bailyn, *The Ideological Origins of the American Revolution*, Cambridge (U.S.), 1967.

7 E. Denninger, *Stato di prevenzione e diritti dell'uomo*, in *Nomos*, 2, 1996, 47 ss. G. Morbidelli, *La Costituzione*, in G. Morbidelli-L. Pegoraro-A. Reposo-M. Volpi, *Diritto pubblico comparato*, Torino, 2007, 42 ss.

8 K. Vašak, *Pour une troisième génération des droits de l'homme*, in C. Swinarski (ed.), *Etudes et essais sur le droit international humanitaire et sur les principes de la Croix-Rouge en l'honneur de Jean Pictet*, The Hague, 1984; S.M. Helmons, *La quatrième génération des droits de l'homme*, in M. Verdussen, *Les droits de l'homme au seuil du troisième millénaire: mélanges en hommage à Pierre Lambert*, Brussels, 2000; A. Alessandri, *Commento al draft di Protocollo sulla ricerca biomedica*, in *I diritti dell'uomo - cronache e battaglie*, 2, 2003; *contra* P. De Stefani *I diritti umani di terza generazione*, in *Aggiornamenti sociali*, 1, 2009. The Author Consider the fourth generation of rights a simple development of the previous ones.

fundamental rights alike.

Faced with this challenge, the legal systems reacted by adopting new fundamental Charters (as the European Charter of Fundamental Rights also called Treaty of Nice) affirming both traditional freedoms and new rights related to bioethics and digital technologies, altogether with an extensive re-interpretation of the previous rights by the Constitutional or Supreme Courts.

Although privacy is a product of earlier centuries, we now live in an age of personal information. It is therefore not surprising that privacy underwent the afore mentioned re-shaping process, gradually shifting from the "right to be left alone" to the actual "data protection" or "data privacy"[9]. Undoubtedly, the digital infrastructure represents an essential element to the modern study of privacy[10]. The rapid uptake of this new information technology by government agencies and companies generated the fear that secret surveillance by states and/or commercial entities could negatively affect individuals' privacy and freedoms. Moreover, it is increasingly obvious that also democratic mechanisms are affected by the procedures in which this information is gathered and exploited[11].

Nevertheless, privacy continues to have an elusive content that frustrates every attempt to define it exhaustively, without questioning the necessity of its protection and regulation[12]. At the same time, it can be noted that the protection of individuals' privacy and data has increasingly been associated with the rights to dignity and self-determination of every human being[13]. These appear to be the new core values of the data protection legislation, and they seem to be particularly suited since they both potentially involve many different aspects of human life[14].

The technological revolution has also accelerated the transition to a global (digital) society, thus rising a wide range of "transnational" issues, including those regarding

---

[9] S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

[10] S. Rodotà, *Tecnologia e diritti*, Bologna, 1995, 19.

[11] Emblematic are Obama's and Trump's presidential campaigns, during which they massively resorted to digital data, even though by different means. E.D. Hersh, *Hacking the Electorate*, Cambridge, 2015; S. Issenbeg, *A More Perfect Union: How President Obama's Campaign Used Big Data to Rally Individual Voters*, in *MIT Technology Review*, 2012; T.E. Frosini, *Tecnologie e libertà costituzionali*, in G. Comandè-G. Ponzalli (a cura di), *Scienza e diritto nel prisma del diritto comparato*, Milano, 2004, 189 ss.; S. Rodotà, T*ecnopolitica. La democrazia e le nuove tecnologie delle comunicazioni*, Roma-Bari, 1997.

[12] As highlighted by A.F. Westin, *Privacy and Freedom*, New York, 1967, 1. Other scholars consider privacy a multiform concept such as an umbrella covering different interests (C. De Giacomo, *Diritto, libertà e Privacy nel mondo della comunicazione globale*, Milano, 1999, 16) or a multidimensional right (T. M. Ubertazzi, *Diritto alla privacy, natura e funzioni giuridiche*, Padova, 2004, 76). Justice Brandeis himself defined privacy as the widest right in *Olmstead v. United States* (277 U.S. 438). However, Norberto Bobbio considered that Law should protect rights rather than question their justification, see N. Bobbio, *op. cit.*, 16-18.

[13] E. Brugiotti, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico,* in Dirittifondamentali.it, 2, 2013, 4.

[14] V. Ricciuto, *Le finalità del Codice*, in V. Cuffaro-R. D'Orazio-V. Ricciuto (a cura di), *Il codice del Trattamento dei dati personali*, Torino, 2007 and S. Rodotà, *Tra i diritti fondamentali ed elasticità della normativa: il nuovo codice della privacy*, in *Europa e diritto privato*, 2, 2004; S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

personal data circulation and exploitation[15]. Such phenomenon urged the states to resort to intergovernmental legal instruments in order to overcome the narrow limits of territorial boundaries[16].

But when did actually start "the race" to privacy?Scholars commonly agree that privacy made its first appearance between the XVIII and XIX centuries, a period known as the private law golden age[17]. Those were also key years for drawing the actual line of cleavage between public and private legal spheres, where the first was deputed to recognize fundamental rights limiting the State powers, and the latter was intended to regulate the relationships between private parties[18].

Due to the rapid urbanization, the diffusion of portable cameras and the changing newspapers-reading habits (yellow journalism, gutter press etc.), the increasingly individualistic western society was more and more sensitive to the need of preserving its intimacy[19]. Soon the Bourgeoisie started to ask for the recognition of a new, yet undefined, right to protect one's private life from such threats[20].

Despite having faced the same social issues, the Common and Civil lawyers, perpetuating their historic dichotomy, related the new-born right to privacy to different fundamental rights, respectively: Liberty and Dignity[21]. This divide can still be seen nowadays as both sides of the Atlantic seems far from finding a solid common ground[22].

---

15 U. Pagallo, *La tutela della Privacy negli Stati Uniti D'America e in Europa*, Milano, 2008, 31; C. De Giacomo, *Diritto, libertà e Privacy nel mondo della comunicazione globale*, Milano, 5; S. Niger, *Privacy e tutela globale*, in *Diritto.it,* October 2000. For an European regulations overview see http://www.privacy.it/normativeu.html.

16 G.M. Flick, *Prefazione*, in G. Santaniello (a cura di), *La protezione dei dati personali*, Padova, 2005; E. Malfatti, *Modelli e prassi di tutela dei diritti fondamentali, in Europa: un punto di vista italiano*, January 2008.

17 M. Perrot, *Modi di* abitare, in P. Ariès-G. Duby (a cura di), *La vita privata*, Roma-Bari, 2001, V, 10; L.M Austin-D. Klimchuk (eds.), *Private Law and the Rule of Law*, Oxford, 2014; W. Lucy, *The Rule of Law as the Rule of Private Law,* in *Private Law and the Rule of Law,* Oxford, 2014, 46 ss.; K.S. Ziegler, *Human Rights and Private Law: Privacy as Autonomy*, London, 2007.

18 The German Public Law school conceived law divided between private law, regulating the relationship between private parties, and public law, which regulated power relationship, see G. Peces-B. Martinez, *Teoria dei diritti fondamentali*, Milano, 1993, 618 ss.; see also S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, cit., 11-30; R. Christen-A. Fischer-Lescano, *Das Ganze des Recht, vom hierarchischen zum reflexiven Verständnis deutscher und europäischer Grundrechte*, Berlin, 2007, 619; J. Ballarin Irinbarren, *Derechos Fundamentales y relaciones entre particulares (la "Drittwirkung" en la jurisprudencia del tribunal Constitucional)*, in *Revista Española de Derecho Constitucional*, 24, 1988, 285-288.

19 In particular, the mass-urbanization enabled the still local media to reach more users, hence compromising someone's reputation became increasingly easier. L. Miglietti, *Profili storico-comparativi del diritto alla privacy*, in *DirittiComparati.it*, 4 December 2014; N. Bobbio, *Liberalismo e democrazia*, Milano, 2011, 35 ss., P. Malvestiti, *Lo Stato e l'economia*, Roma, 1955, 21 ss.

20 In my opinion, the bourgeoise's call for more privacy could be related to its new political role in the liberal States institutions, which drew upon it the interest of the press and, later on, other media. See also D. Diderot, *Potere politico e libertà di stampa*, Roma, 1966; P. Maltese, *Stampa e potere: storie di censura giornalistica*, Catania, 2017.

21 This situation is summarized by James Whitman, *The Two Western Cultures of Privacy: Dignity v. Liberty*, in *Yale Law Journal*, 113, 2004, 1151-1221; see also J.L. Halpérin, *L'essor de la "*privacy*" et l'usage des concepts juridiques*, in *Droit et Société*, 61, 2005, 765 ss.

22 F. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in *Boston College Law Review*, 48, 2007; C.J. Bennett, *In Defense of Privacy: the Concept and the Regime*, in *Surveillance and Society*, 8, 2011, 485 ss.; D.L. Baumer-J.B. Earp-J.C. Poindexter, *Internet and Privacy Law: A Comparison between United States and the European Union*, in *Computers & Security*, 5, 2004, 400 ss.

Yet, not only the public opinion, but the very scholars believe that *privacy*, irrespectively of its name (privacy, *vie privée*, *riservatezza*, *intimidad*, *Privatsphäre etc.*), still shares the same meaning, or better, purpose. Many scholars assumed this being the consequence of American privacy legal transplant all around the world[23]. This is not surprising, if we consider that most academics consider the famous 1890 article "*Right to Privacy*", written by the Bostonian lawyers Samuel Warren and Louis Brandeis[24] on the Yale Law Journal, the first legal debut and the cornerstone of modern privacy. Nevertheless, it must be noted that their work didn't came out of thin air, instead it was the brilliant synthesis and development of both the English and French experiences, unfortunately often overlooked[25].

Indeed, there are numerous elements supporting the theory of a "double independent origin" of privacy, as opposed to the circulation, if not transplant, of the American experience. This explains why it took the United State more than 70 years to transpose it from the "books" to actual case law or statues[26], and, also, why American thriving academics constantly related to privacy both private law key institutes and fundamental rights as freedom and human dignity[27]. The first revolves around Common law's notion of property and freedom from the State, whilst the latter is likely to have come from the *Ancien Régime*'s notion of honor[28].

As we will see, this mix granted the United States to legitimately be the international leader in privacy protection, especially during the '60s, until their substitution by the EU.

1.1. The English Common law and the right to "propercy"

In light of the fact that private law is the backbone of English legal and political life,

[23] J.J. Halpérin, *L'essor de la "*privacy*" et l'usage des concepts juridiques*, cit., p. 765-782. For an analysis in depth of the legal transplant process see A. Watson, *Legal Transplants: An Approach to Comparative Law*, Athens (U.S.), 1974.

[24] S.D. Warren-L.D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, 4, 1890, 4, 193 ss.

[25] *Ibid.*

[26] *Griswold v. Connecticut,* 381 U.S. 479 (1965). The Executive Director of the Planned Parenthood League of Connecticut, and its medical director, were convicted as accessories for giving married persons information and medical advice on how to prevent conception and prescribing a contraceptive device or material for the wife's use. A Connecticut statute made it a crime for any person to use any drug or article to prevent conception. Appellants claimed that the accessory statute violated the Fourteenth Amendment. Since the right to privacy is not mentioned in the Constitution, Justice Douglas needed to find another basis for it. He argued somewhat vaguely that the "penumbras" surrounding many of the constitutional amendments, like the Fifth Amendment (protection against self-incrimination), suggested that the right to privacy from the state can be inferred as something that the Constitution is intended to protect. Instead Arthur Joseph Goldberg and John Marshall Harlan II concurring opinions assumed that privacy was protect either by the 9th or 14th Amendments. However, Justice Black's dissenting opinion firmly warned against the risks of resorting to a "large, abstract, ambiguous" concept of privacy. See also E. Zoller, *Grands arrêts de la Cour suprême des États-Unis*, in *Droit fondamental*, 2000, 694.

[27] R.C. Post, *Three Concepts of Privacy*, in *Georgetown Law Journal*, 89, 2001, 2087 ss.

[28] J.L. Halpérin, *Protection de la vie privée et privacy : deux traditions juridiques différentes*?, in *Nouveaux Cahiers du Conseil constitutionnel*, 48, 2015.

it is not surprising that Common lawyers have associated privacy with property, by defining it as *ius excludendi alios*[29]. Nevertheless, English society started a relentless process of property "dematerialization", by adopting a copyright regulation meant to protect property from behaviors unrelated to its material retention[30].

Therefore, the bourgeoisie tried to regulate property's new "inner dimension" (the unborn privacy) by resorting to the same remedies devoted to protecting its physical nature and economic exploitation[31]. This outcome was facilitated by judges generally granting injunctions on the ground of breach of contract, copyright infringement, abuse of confidence and physical trespass.

However, English courts faced many difficulties while trying to overextend property legal boundaries. For instance, when dealing with wrongful publication related cases, the judiciary tried not to discriminate between the different rights of property belonging to the author of a published book and of an unpublished manuscript. Yet, the first one is the right to profit from publication, the second one is the right to decide whether there should be any publication at all. What if the wrongful publication injunction concerned a document intended to remain private and never to be published, as a personal letter? In this case the right infringed could not have been arguably associated with a Copyright, that is essentially meant to grant primacy over its economic use. Property soon became increasingly narrow, thus urging the judiciary to simultaneously rely on remedies other than the breach of confidence or contract.

In *Prince Albert v. Strange* (1849)[32], despite recognising right to ownership of etchings sufficient to justify the issuance of the injunction, Lord Cottenham stated that he was bound to assume that the possession of the etchings by the defendant had «its foundation in a breach of trust, confidence, or contract»[33] and that upon such ground also the plaintiff's title to the injunction was fully sustained. The court upheld that common law rule prohibited not only the reproduction of the etchings made for the costumer's own pleasure, but also the publishing of their description also in the form of a catalogue. According to Lord Cottenham, a man «is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his» and declared that «privacy is the right invaded»[34], which made its first appearance in a Common law ruling.

We can find a similar argument in *Yovatt v. Winyard* (1820) where an injunction was granted against making any use of or communicating certain recipes for veterinary medicines written in a personal diary the defendant had surreptitiously got access to. Lord Eldon «granted the injunction, upon the ground of there having been a breach

[29] Notably, property framed both the relationships among privates and the political affiliation, at least prior to the appearance of political parties, see A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, 48.

[30] The very first copy regulation has been the 1710 Statue of Anne, later replaced by the 1988 Copyright, Design and Patents Act.

[31] A. Baldassarre, *op. cit.*

[32] *Prince Albert v. Strange*, 1 McN. & G. 25 (1849).

[33] Lord Cottenham in *Prince Albert v. Strange*, 1 McN. & G. 23, 43 (1849).

[34] *Ibid.*

of trust and confidence»[35], despite the fact that it was difficult to draw any sound legal distinction between such a case and one where a mere stranger wrongfully obtained access to the book. Again, in *Pollard v. Photographic Co.* (1888)[36], the court, while expressly finding the breach of both contract and trust sufficient to justify its interposition, felt the necessity to base its decision also upon the right of property[37].

Instead, in *Tuck v. Priester* (1887)[38], the plaintiffs owned a picture and employed the defendant to make a certain number of copies. However, the latter made a greater number of copies to later sell them at a lower price. The Lords Justices' statements differed as regards the application of the copyright acts to this case, but held unanimously that independently of those acts, the plaintiffs were entitled to an injunction and damages solely for breach of contract.

Up until now the afore mentioned cases concerned a tangible document, whether it was a photo or a writing. What if the wrongful publication didn't concern a manuscript, a document or an artwork, but a personal information or an unwritten speech? In *Abernethy v. Hutchinson* (1825)[39], the plaintiff, a distinguished surgeon, sought to restrain the publication of some unpublished lectures which he had delivered at St. Bartholomew's Hospital in London. In this case Lord Eldon doubted whether a property right on unwritten lectures could exist, yet he granted the injunction on the ground of breach of confidence.

To sum it up, the English courts started affording protection to thoughts, sentiments and emotions, as long as they were expressed through arts or writings, by preventing their publication and circulation when they were not permitted through copyright. They clearly intended to use property in no other sense than protecting mere interest or feeling, and to describe a substantial right of legal interest. Finally, when the copyright started being insufficient, the judiciary began granting injunctions solely on the ground of breaches of trust, contract or confidence. The dissociation between the concepts of property and privacy was the necessary precondition for the subsequent configuration of an autonomous individual right to be let alone.

However, in the long run private law has proved not to protect fundamental rights sufficiently because of its arbitrary nature and the potentially different economic "weight" of the parties[40]. The public law intervention became, therefore, necessary[41],

---

35 *Yovatt v. Winyard*, 1 J. & W. 394 (1820).

36 *Pollard v. Photographic Co.*, 40 Ch. Div. 345 (1888) a photographer who had taken a lady's photograph under ordinary circumstances was restrained from exhibiting and selling copies of it, on the ground of both breach of an implied term in the contract and of confidence.

37 *Duke of Queensberry v. Shebbeare* (1758), 2 Eden 329; *Murray v. Heath*, 1 B. & Ad. 804 (1831); *Tuck v. Priester*, 19 Q.B.D. 629 (1887).

38 *Tuck v. Priester*, 19 Q. B. D. 639 (1887) The plaintiffs registered the copyright in the picture and then brought suit for an injunction and damages.

39 *Abernethy v. Hutchinson*, 1 H. & TW. 28 (1825).

40 M.J. Radin, *Boilerplate: A Threat to the Rule of Law?*, in *Private Law and the Rule of Law,* Oxford, 2014, 300 ss.

41 L.M. Austin-D. Klimchuk,(eds.), *Private Law and the Rule of Law*, Oxford, 2014; W. Lucy, *The Rule of Law as the Rule of Private Law,* in *Private Law and the Rule of Law,* Oxford, 2014, 46 ss.; K.S. Ziegler, *Human Rights and Private Law: Privacy as Autonomy*, London, 2007.

and it is partially responsible for the recent private law shift from property right to personal right[42].

1.2. The French experience: who's copying who?

Since 1789 Revolution, the distinction between private and public life have been at the centre of a many-sided debate. Despite an early awareness of privacy, triggered by many cases of libel by newspapers, the French legislator did always hesitate to provide a clear definition of private life, thus leaving its interpretation to the discretion of the courts[43].

During the Ancien Régime, in the absence of a criminal code, perpetrators of violations undermining the public order or people's reputation were sanctioned by the Tribunal of Public Opinion, on the ground of academic works such as the *Traité des injures dans l'ordre judiciaire* (1776)[44] or the *Répertoire universel* (1778). In this period an ample literature flourished, inspired by different contingency factors such as the «*causes célèbres*»[45], the smear campaign against Queen Marie-Antoinette[46] or the very Beaumarchais's plays[47]. Altogether these elements suggested an increasing awareness of privacy protection[48].

After the 1789 Revolution, the press enjoyed a boundless freedom (all the press crime had been repealed), resulting in many civil litigations for defamatory writings[49]. However, on 18 July 1791 the Champ du Mars shootings and Louis XVI's escape attempt urged the founding fathers to adopt a statue prohibiting any act encouraging civil disobedience[50]. Nevertheless, they rejected any further restriction on the freedom of expression except for defamation. When questioning public servants' integrity or common people's private life, the press enjoyed the *exceptio veritatis* (exception of the truth),

---

[42] P. Rescigno, *Trattato di diritto privato*, Torino, 1982, 236; N. Ferreira, *Fundamental Rights and Private Law in Europe: The Case of Tort Law and Children*, Abingdon-New York, 2011, 21 ss.

[43] H. Blin-A. Chavanne-R. Drago, *Traité du droit de la presse*, Paris, 1969, 275.

[44] Dareau harshly condamned libels, slanders and defamations (without clearly distinguishing them). He referred to a 1571 *déclaration royale* sanctioning those who had published books with the solely objective to libel someone. He wrote that libels could harm even a king «*en le faisant descendre du Trône à la vie privée*», however private life had not yet a legal definition. F. Dareau, *Traité des injures dans l'ordre judiciaire*, Paris, 1776, IX, 4, 7-8, 27.

[45] Cases involving public figures and presenting both a public and private dimension. S. Maza, *Vies privées, affaires publiques. Les causes célèbres de la France pré-révolutionnaire*, translated by C. Beslon-P.E. Dauzat, Paris, 1997, 304.

[46] S. Burrows, *Blackmail, Scandal and Revolution. London's French Libellistes, 1758-1792*, Manchester, 2006, 147.

[47] Slander has indeed an important role in his play "*Le Barbier de Séville"* as noted by J.L. Halpérin, *Diffamation, vie publique et vie privée en France de 1789 à 1944*, in *Droit et Cultures*, 65, 2013.

[48] C. Walton, *Policing Public Opinion in the French Revolution. The Culture of Calumny and the Problem of Free Speech*, Oxford, 2009, 39.

[49] J.L. Halpérin, *Diffamation, vie publique et vie privée en France de 1789 à 1944*, cit., 145 ss.

[50] C. Walton, *Policing Public Opinion in the French Revolution. The Culture of Calumny and the Problem of Free Speech*, Oxford, 2009, 109.

that was expressly designed to exclude any allegation as long as established facts were concerned. The Truth, it doesn't matter how regretful or unpleasant it was, was not considered to be a threat for ordinary people's integrity except for the "perverts"[51].
The Napoleonic parenthesis left civil and criminal codes protecting family secrets and limiting the press freedom., on the ground that every individual exerted a property right over his own reputation[52].
In 1819 the three statues "de Serre" — named after Louis XVIII's Keeper of seals — intended to liberalise the press once more and for the first time discerned between defamation and insult[53]. The 1819 Acts, together with Royer-Collard's famous speech, further developed the idea that honour and reputation[54] belong to the individual. De Serre stated «*tout, dans une famille, peut n'être pas irréprochable; c'est qu'il est des plaies cachées, des hontes secrètes, et que la loi a dû défendre absolument toute recherche indiscrète à cet égard*»[55]. Royer-Collard declared that «*n'est pas permis de dire la vérité sur la vie privée*» and also «*voilà donc la vie privée murée, et si je puis me servir de cette expression, elle est déclarée invisible, elle est renfermée dans l'intérieur des maisons*»[56]. From now on the *exceptio veritatis* applied only to indiscretions referred to public servants, considered benefitting society. Nonetheless, if the allegations concerned a public servant private life the protection level decreased. In this case it was settled case-law that representatives and public servants could also appeal to the Court d'assise for private life matters enjoying the *exceptio veritatis* as the commoners (the theory of "divisibility" or "wall"). The Same applies to the 1868 Act, that sanctioned the disclosure of any private information unauthorised by the concerned subject. The French divide between the private and public spheres — opting for a stronger protection of private life for both private and public figures — was not unanimously welcomed by the commentators. It is important to notice that while Warren and Brandeis were praising the protection accorded to privacy by French legislation, on the other side of the Ocean Laboulay was criticizing it and commending the American freedom of expression. The grass is always greener[57].
However, the legislator did not define the exact content of the "private life" concept. It resulted in a wider margin of appreciation by the courts with reference to the recognition of the exception of truth[58]. As a consequence, the courts determined the competence of the *Assise* over the Correctional tribunal and *viceversa* depending on whether the case was related to public functions or to private life and on whether or not it concerned a public servant or a private.

---

[51] Loi Le Chapelier du 20 juillet 1791, Art. 17, Judiciary chapter. See also F. Gauthier, *Triomphe et mort du droit naturel en Révolution (1789-1795-1802)*, Paris, 1992, 310.

[52] Directoire Exécutif, *Réimpression de l'ancien Moniteur,* Paris, 28, 1858, 685, J.L. Halpérin, *Diffamation, vie publique et vie privée en France de 1789 à 1944*, cit.

[53] 17 may 1819 Act, at Art. 13.

[54] The first as self-esteem, the latter the opinion of others.

[55] *Archives parlementaires,* 2e série, tome XXIV, 28 avril 1819, 93.

[56] *Ibid.,* 71-73.

[57] René Lefebvre (pseudonyme de Laboulaye), *Paris en Amérique*, Paris, 1887, 136.

[58] For a in depth analysis of the jurisprudence see J.L. Halpérin, *Diffamation, vie publique et vie privée en France de 1789 à 1944*, cit., 145 ss.

Only in 1874 the *Cour de cassation*, tried to define private life content with a decree (*arrêt*). The Court of Appeal of Dijon had condemned a newspaper for revealing the name of the participants to a pilgrimage to Notre-Dame d'Estang. The decree extended the concept of private life outside the domestic walls, covering every fact belonging to the «*domaine du for intérieur*» or «*liberté de conscience*»[59]. Afterwards, the 1881 Act, despite seeming to restate the same 1819 Acts principles, eventually resulted in the fall of the "wall" between the public and private spheres, enabling to look through. However, this applied only to public figures as artist, politicians, etc. This change paved the way to a new privacy evolution during the 60's and 70's, in order to protect also celebrities' private life, in line with the American example.
Finally, we can observe that also the French cultural tradition followed a path similar to the English one, by alternating different privacy designs and mixing what Robert Post described as the three Common law concepts of reputation, namely: property, honour and dignity.

1.3. The birth and expansion of American privacy

Despite their early awareness, both the UK and France neither did recognize privacy as an autonomous right[60], nor did determine its content. However, they are the stepping stones upon which Warren and Brandeis had been able to leap towards modern privacy. Their writing "The Right to Privacy" is a milestone in privacy protection, as it represents the first legal paper recognizing it as a separate right. Until then private life protection struggled to be recognised by the legal system, running into the hostility of both scholars and courts, who were willing to associate it to other rights as property, honour and reputation[61].
As soon as new devices and business practices (portable cameras and gossip press) started threatening the person in unpredicted ways, the society deeply felt the urge to secure what Judge Cooley defined as the right «to be left alone»[62]. Therefore, the Bostonian lawyers, appealing to the common law "eternal youth" and capability to adapt to changing times, tried to carve it from within the existent American legal system[63].
The authors argued that so far privacy had been partially protected within unconven-

[59] J.L. Halpérin, *Protection de la vie privée et privacy : deux traditions juridiques différentes ?,* in *Les nouveaux cahiers du Conseil constitutionnel*, 48, 2015; Id., *Diffamation, vie publique et vie privée en France de 1789 à 1944*, cit.

[60] *The Right to Privacy in Nineteenth Century America*, in *Harvard Law Review*, 1981, 94, 1892 ss.

[61] A. Westin, *Privacy and Freedom*, New York, 1967, 337; A. Baldassarre, *op. cit.*, 16.

[62] T.M. Cooley, *A Treatise on the Law of Torts, or the Wrongs which arise Independent of Contract*, Chicago, 1888, 29. Around the same time that Warren and Brandeis published their article, the Supreme Court referred to the right to be let alone in holding that a court could not require a plaintiff in a civil case to submit to a surgical examination: «As well said by Judge Cooley: 'The right to one's person may be said to be a right of complete immunity; to be let alone», in *Union Pac. Ry. Co. v. Botsford*, 141 U.S. 250 (1891). However, it must be noted that Cooley's right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy see R.E. Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Providence, 2004, 128.

[63] See A. Baldassarre, *op. cit.,* 40.

tional property claims[64], the remedies of which started falling short to address injury other than tangible[65]. It was a necessary step to dismiss any direct correlation with property, and link privacy to the personal inviolability[66]. Consequently, privacy ceased to be a property "distortion" bound by the economic nature of its infringement and started deserving protection solely for the relevance to its holder[67]. It is fair to say that the article did not only separate privacy from property, slander and libel[68], it also suggested a new legal perspective, where personal values stood over economical ones[69]. Yet the Bostonian lawyers still conceived privacy violation as civil wrong (a tort)[70], *ergo* failing to leave the private law's logics behind.

Not to mention, at the time of its publishing the "Right to Privacy" found a society still unprepared to dismiss completely any association with property. For instance, in the case *Roberson v. Rochester Folding Box Co.* the New York Appeal Court refused to afford protection to the right of privacy arguing that there was no precedent for such an action to be found[71]. However, just a few years later the Supreme Court of Georgia, in *Paveish v. New England Life Insurance Company*[72], started acknowledging privacy. Afterwards, the ruling was followed by an increasing number of decisions.

In 1939 Warren and Brandeis's formulation was finally enshrined by the eminent torts scholar William Prosser in the *Restatement of Torts*[73]. Still the "harboring" of privacy in the U.S. Constitution had yet to come. *Olmstead v. United State*s (1928)[74] highlighted the need for conceptualizing a flexible fundamental right to privacy. In fact, the Court held that the wiretapping of a person's home telephone (done outside a person's house) did not run afoul of the Fourth Amendment because it did not involve a trespass inside a person's home. The strict decision was overruled only in1967 by *Katz v. United States*[75].

---

[64] Such as defamation, breach of trust or confidence, or breach of implied contract, all examples afore mentioned.

[65] S.D. Warren-L.D. Brandeis, *op. cit.*, 191; see also N.L. Richards, *The Limits of Tort Privacy*, in *Journal on Telecommunications and High Technology Law*, 9, 2011, 357-360.

[66] S. Rodotà-P. Conti (a cura di), *Intervista su privacy e libertà*, Roma-Bari, 2005, 8-9.

[67] U. Pagallo, *La tutela della privacy negli Stati Uniti d'America ed in Europa*, Milano, 2008, 64-65; See also A. Baldassarre, *op. cit.*, 18; G. Alpa-B. Markesinis, *Il diritto alla privacy nell'esperienza di common law e nell'esperienza italiana*, in *Rivista trimestrale di diritto civile e procedura civile*, 51, 1997.

[68] Defamation protected from injuries to reputations, whilst privacy addressed an "injury to the feelings," a psychological form of pain that was difficult to translate into the tort law of their times, which focused more on tangible injuries. S.D. Warren-L.D. Brandeis, *op. cit.*, 196.

[69] S. Rodotà, *Tecnologie e diritti*, cit., 23.

[70] For an analysis of torts see L. Moccia, voce *Common Law*, in *Digesto Discipline Privatistiche*, *Sezione Civile*, III, 1988, 27 ss.; U. Mattei, *Il diritto angloamericano*, in R, Sacco, *Trattato di diritto civile*, Torino, 1992, 332 ss.; A. Gambaro-R. Sacco, *Sistemi giuridici comparati,* in R. Sacco (a cura di), *Trattato di diritto comparato*, Torino, 2008.

[71] *Roberson v. Rochester Folding Box Co.,* 64 N.E. 442, 171 N.Y. 538 (1902).

[72] *Paveish v. New England Life Insurance Company* 122 Ga. 190, 50 S.E. 68 (1905).

[73] N.L. Richards, *The Limits of Tort Privacy*, cit., 363-364. U.M. Ubertazzi, *Diritto alla privacy, natura e funzioni giuridiche*, cit.

[74] *Olmstead v. United State*s 277 U.S. 465 (1928). Justice Louis Brandeis vigorously dissented, chastising the Court for failing to adapt the Constitution to new problems: «In the application of a Constitution, our contemplation cannot be only of what has been, but of what may be», at 474.

[75] *Katz v. United States*, 389 U.S. 347 (1967).

Indeed, Warren and Brandeis's aim was to explore privacy's roots and to focus on the existing common-law torts inadequacy, rather than providing a comprehensive conception of it[76]. As a consequence, even though the "right to be alone" was mentioned in many decisions, it remained a vague concept[77]. Moreover, the legislator's hesitancy compelled commentators and courts to attempt a definition more extended than mere solitude[78]. Privacy has indeed a cross-cutting nature, hence some commentators preferred to consider it as set of different ideas, rather than a unitary right[79]. According to Godkin, privacy included the right to keep one's own affairs for himself and to decide to what extent share them[80]. This has raised some concerns with regard to the amount of control that every individual should have over the access to the self. Indeed, «not all privacy is chosen. Some privacy is accidental, compulsory, or even involuntary»[81]. Ruth Gavison, in an attempt to address these shortcomings equated privacy to "limited access", by which the commentator meant «three independent and irreducible elements: secrecy, anonymity, and solitude»[82]. However, this definition could be too limited, as current information collection, storage, and computerization often do not directly harm secrecy, anonymity, nor thwart solitude[83].

---

[76] E.J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *New York University Law Review*, 39, 1964, 970 ss.

[77] D.M. O'Brien, *Privacy, Law, and Public Policy*, New York, 1979, 5; T. Gerety, *Redefining Privacy,* in *Harvard Civil Rights-Civil Liberties Law Review*, 12, 1977, 263 ss.

[78] D.M. O'Brien, *ibid*., 5; T: Gerety, *ibid*., 263 ss.; A.C. Breckeridge, *The Right to Privacy*, Lincoln, 1970, 1 («Privacy, in my view, is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others»); D.J. Solove, *Conceptualizing Privacy*, in *California Law Review*, 90, 2002, 1103 ss.

[79] Judith Thomson, claims that the right to privacy is not a distinct right, but it is «overlapped by other rights» J.J. Thomson, *The Right to Privacy*, in F. Shoeman (ed.) *Philosophical Dimension of Privacy: an Anthology*, Cambridge, 1984, 284, whilst Jerry Kang defines privacy as the union of three overlapping clusters of ideas: physical space «the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals»; choice «an individual's ability to make certain significant decisions without interference»; flow of personal information «an individual's control over the processing-i.e., the acquisition, disclosure, and use-of personal information»; J. Kang, *Information Privacy in Cyberspace Transactions*, in *Stanford Law Review*, 50, 1998, 1202-03.

[80] The individual has the «right to decide how much knowledge of [a person's] personal thought and feeling…, private doings and affairs... the public at large shall have»; E.L. Godkin, *The Rights of the Citizen, IV. To His Own Reputation*, in *Scribner's Magazine*, 8, 1890, 65; see also E.L. Godkin, *Libel and Its Legal Remedy,* in *Journal of Social Science*, 12, 1880, 69, 80. Similar, yet more detailed Ernest Van Den Haag's theory, according to which privacy was an exclusive access to nothing less than «a realm of his own. The right to privacy entitles one to exclude others from (a) watching, (b) utilizing, (c) invading (intruding upon, or in other ways affecting) his private realm»: see E. Van Den Haag, *On Privacy*, in J.R. Pennock-J.V. Chapman (eds.) *Nomos XIII: Privacy,* New York, 1971, 149.

[81] D.M. O'Brien, *Privacy, Law, and Public Policy*, cit., 15, see also D.J. Solove, *Conceptualizing Privacy*, cit., 1104.

[82] «Our interest in privacy is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. privacy as limited access to the self is valuable in furthering liberty, autonomy, and freedom»: see R. Gavison, *Privacy and the Limits of Law*, in *Yale Law Journal*, 89, 1980, 423.

[83] However, Ruth Gavison considers that modern data processing falls within her conception the collection, storage, and computerization of information falls within her conception. R. Gavison, *Ibid*., 436; D.J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, in *Stanford Law*

Another theory argues that privacy consists of two elements: the interest in being left alone and the interest in concealing information, rather than limiting its access[84]. The idea of concealment has clearly inspired American *Information privacy*, a fundamental right set in law-case by the Supreme Court of the United State and carved directly from the fourth Amendment[85]. It allows to protect both the individual's interest in making decisions autonomously and in avoiding disclosure of personal matters. However, information privacy is characterized by a relevant limitation: it requires the absolute secrecy of the information to be invoked. Once the fact is divulged, no matter how little, it no longer deserves such a protection[86]. This led to the so called "third party doctrine", which has its beginning point in *Katz v. United States*[87]. In *Katz*, the Court held that wiretapping of telephone calls made in a public telephone booth constituted a search and thus required a warrant. Up until then, to be considered a search under the Fourth Amendment, searches had to occur inside someone's home and required a physical intrusion. In rejecting the Government's argument that such precedents should apply, the Court countered that «the Fourth Amendment protects people, not places» and that what a person «seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected»[88]. Therefore, a person's individual expectations of privacy should affect the substantive reach of her Fourth Amendment protections[89].

However, according to this theory the Fourth Amendment still doesn't apply to personal information shared with a third party, such as banks or telephone companies, for no secrecy should be expected by the subject in this case[90]. Beyond possession of this information by the privates parties, what really looms is the threat of government access to these data without a warrant, unless their secrecy is assured by a specific statue[91]. Furthermore, Fourth Amendment jurisprudence did not evolve to compensate for the increasing amount of personal information shared daily, continuing to apply the third party doctrine.

As noted by Edward Bloustein and Arnold Simmel, such feature excludes any form of group privacy, even when the amount of people the information is shared with is

Review, 53, 2001, 1393, 1422.

84 R.A. Posner, *The Economics of Justice*, Harvard University Press, Harvard, 1981, 272-273.

85 *Whalen v. Roe,* 429 U.S. 599-600 (1977), see also *Griswold v. Connecticut,* 381 U.S. 479 (1965) and *Roe v. Wade,* 410 U.S. 113 (1973).

86 For example, in *Katz v. United States*, the Court observed: «What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection» *Katz v. United States*, 389 U.S. 347, 351 (1967); seemingly in *California vs. Greenwood 486 U.S. 35 (1988)* and *Florida v.Riley, 488 U.S. 445 (1989)* because the surveillance was conducted from a public vantage point; see also *U.S. West, Inc. v. Federal Communications Commission.*

87 See *Katz v. United States*, 389 U.S. (1967).

88 *Ibid.,* at 351-52. The *Katz* opinion was quite innovative, in that it was willing to overturn clearly binding precedent in response to social change.

89 See *Katz v. United States*, 389 U.S. (1967) 347; see in particular J. Harlan's concurring opinion at 361.

90 See e.g. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979): «This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties».

91 See D.J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, in *Southern California Law Review*, 75, 2002, 1083 ss.

so little that it doesn't compromise its secrecy nor intimacy[92].

Alan Westin further developed the theories above mentioned, so as to include collective forms of privacy and to soften the limited access boundaries. In fact, he stated «Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others»[93]. Still, privacy cannot revolve around individual prerogative only, instead it is also an issue of what society deems to be appropriate to protect, thus acting before and regardless of any form of control. Hence, Richard Murphy tried to elaborate a neutral approach to privacy, considering protection worthy with respect to «any data about an individual that is identifiable to that individual»[94], which is very similar to the "personal data" definition made by Directive 95/46/EC regulating European data flows. Nonetheless, some commentators addressed personal information use to be limited by the purposes for which the information were given[95]. Thereafter Edward Bloustein linked privacy and personhood directly, arguing that the control over one's own information should be considered the bulwark of self-determination[96]. Correspondingly, any assault to privacy should translate into an attack to human personality or individuality[97].

The Supreme Court has espoused this theory in its substantive due process decisions *Griswold v. Connecticut*[98], *Eisenstadt v. Baird*[99], *Roe v. Wade*[100]. In *Roe v. Wade* the Court defined privacy as an «interest in independence in making certain kinds of important decisions»[101]. This definitely led some commentators to identify privacy as an integral

[92] See, e.g., A. Simmel, *Privacy Is Not an Isolated Freedom*, in J.R. Pennock-J.V. Chapman (eds.), *Nomos XIII: Privacy*, New York, 1971, 71, 81 and E.J. Bloustein, *Individual and Group Privacy*, Brunswick, 1978, 123 ss.

[93] A. Westin, *Privacy and Freedom*, New York, 1967, 7; see R.P. Benzanson, *The Right to Privacy Revisited: Privacy, News, and Social Change*, in *California Law Review*, 80, 1992, 1133, 1135 («I will advance a concept of privacy based on the individual's control of information»); O.M. Ruebhausen-O.G. Brim, *Privacy and Behavioral Research*, in *Columbia Law Review*, 65, 1965, 1184, 1189 («The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others»); see A. Wells Branscomb, *Who Owns Information? From Privacy Public Access*, New York, 1994; C. Fried, *Privacy*, in *Yale Law Journal*, 77, 1968, 483 ss.

[94] R.S. Murphy, *Property Rights in Personal Information. An Economic Defense of Privacy*, in *Georgia Law Journal*, 84, 1996, 2381, 2383.

[95] D.J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, cit., 1439; Id., *Conceptualizing Privacy*, cit., 1108; K.L. Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, in *Law and Contemporary Problems*, 31, 1966, 342-344.

[96] E.J. Bloustein, *Privacy as an spect of human Dignity: An Answer to Dean Prosser*, in *N.Y. Law Review*, 39, 1964, 971; *contra* R. Gavison, *Privacy and the Limits of Law*, in *Yale Law Journal*, 89, 1980, 421-424, who considers the reductionist approach of the first not addressing privacy *per se*, in the absence of other interests, circumstance which leads to a loss of value and protection.

[97] E.J. Bloustein, *ibid.*

[98] *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[99] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).

[100] *Roe v. Wade*, 410 U.S. 113 (1973).

[101] *Whalen v. Roe*, 429 U.S. 589 (1977) at 599-600.

part of our humanity, the very beginning of all our freedoms[102]. As we will see, despite all the aforementioned definitions US privacy regulations address mostly to the State, rather than private actors (corporations, businesses, etc.), struggling to abandon completely the commercial logics limiting privacy to intimate, unpleasant or familiar information. Instead, International and European fundamental Charts did not appear to hesitate to to give to privacy a constitutional status, thus facilitating its protection.
The 1948 Universal Declaration of Human Rights (UDHR) mentions privacy and private life at Art. 12[103]. As a consequence, the UDHR inspired both Art. 17 of the International Covenant on Civil and Political Rights and Art. 8 of the 1950 ECHR. However, the ECHR[104] does not consider it as an absolute right, which means that it can undergo some limitations in order to balance eventually conflicting interests. Nevertheless, it will be up to each Member State to assess such a balance within their margin of appreciation and discretion[105].
Only later, during the second half of XX century, privacy rooted in European courts. Both in France (case Bardot)[106] and Italy (Soraya)[107], the courts accorded public figures a right to have their private life protected from the media. Consequently, the concept of privacy adopted was mirroring the American design as the "right to be left alone". However, its constitutional foundation will be set not, as the U.S. Fourth Amendment, in the freedom from the State, but in human dignity and self-determination.

2. From privacy to data privacy

The digital revolution has deeply affected our reality. We can book an hotel or a flight, purchase books or clothes, share with our "friends" opinions or pictures, all with few "clicks". However, what has been the price for a such more comfortable life?
Every operation *via* digital device requires and produces invisible data. Some are personal (our name, birthdate, address) others are sensitive (sexual orientation, religion,

[102] D.J. Solove, *Understanding Privacy*, Cambridge (U.S.), 2008.

[103] «No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks». The article has been written by a French and American joint committee led by René Cassin-John Humphrey-J.L. Halpérin, *Protection de la vie privée et privacy: deux traditions juridiques différentes ?*, cit., 59 ss.

[104] About the role of the ECHR in EU members legal systems see O. Pollicino-G. Martinico (eds.), *The National Judicial Treatment of the ECHR and EU Laws*, Oxford, 2010. See also P. De Hert-S. Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action*, in S. Gutwirth (ed.), *Reinventing Data Protection?*, New York, 2009, 3; U. Scheuner, *Fundamental Rights in European Community Law and National Constitutional Law*, in *Common Market Law Review*, 12, 1975, 171 ss.; H.C. Kruger-J. Polakiewicz, *Proposal for a Coherent Human Rights Protection System in Europe*, in *Human Rights Law Journal*, 22, 2001, 1 ss.

[105] S. Bartole-P. De Sena-V. Zagrebelsky, *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, 297; G. Parodi, *In tema di bilanciamento degli interessi nella giurisprudenza costituzionale*, in R. Bin-G. Pitruzzella, *Diritto pubblico*, Torino, 1995, 203 ss.; G. Pino, *Il diritto all'identità personale, interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.

[106] *Brigitte Bardot*, Cour d'appel de Paris, 27 February 1967, see *Dalloz périodique*, 1967, 450.

[107] Italian Supreme Court, 27 May 1975, no. 2129.

political affiliation), most of them looks harmless (preferred books and other purchases), nevertheless all of them are "crystalized" in databases of the providers. We should think of the Web as an enormous mining complex, where data are extracted and stored, then transported to the refineries and, once the product has been polished or processed, sold. But beneath the digital ground there is no ore, there are people. It might sound extravagant, but the final product of such a cumbersome process it is nothing but us.

Technological transmuted personal information in an exchangeable commodity, capable of undergoing further level of sophistication[108]. Once "materialized", privacy has become even more vulnerable.

The new millennium has seen the occurrence of two radical changes. On one hand the 9/11 started a worldwide military campaign against terrorism, urging the governments to continuously look for new means of surveillance, so to successfully conduct counterterrorist operations. On the other, firms and companies are exploiting personal data for economic gains, profiling the customers in order improve their marketing practices. As a result, the market itself is pushing for the creation of more intrusive devices and software. Personal data have become «the new currency of the digital world»[109].

At the end of XX century the Legislators considered sufficient to protect privacy though legal instruments. Therefore, the U.S. and EU alike started adopting an increasing number of regulations. However, they could not hope to cope with the fast pace imposed to the digital revolution by the market. An example is given by the definition of protected data. Originally only personal data transfer was hindered, but now specific algorithms enable the data brokers (new commercial figure) to obtain the very same protected information starting from unprotected data.

2.1. Data privacy in the U.S.

During 1970 the rapid uptake of computerized databases and devices by companies and government agencies sparked fears of potentially harmful effects for individual freedoms. Secret surveillance by the State or commercial entities[110], errors in the data etc. were perceived as new threats to the private sphere. As a result, data protection legislation made its appearance firstly in the U.S and later in Europe[111]. During the second half of the XX century, thanks to its technological advantage over the rest of the world, Washington took the lead in data protection, only to be followed (and now

[108] S.E. Dorraji-M. Barcys, *Privacy in Digital Age: Dead or Alive? Regarding the New EU Data Protection Regulations*, in *Social Technologies*, 4, 2014, 306 ss.

[109] M. Kaneva in S.E. Dorraji-M. Barcys, *Privacy in Digital Age: Dead or Alive? Regarding the New EU Data Protection Regulations*, cit., 306; see also M. Bassini-L. Liguori-O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi*, in F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 333 ss.

[110] See *Nader v. General Motors Corp.* 25 N.Y. 2d 560 (1970).

[111] F.H. Cate, *The EU Data Protection Directive, Information Privacy and the Public Interest*, in *Iowa Law Review*, 80, 1995, 431-433; P.M. Regan, *Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations*, in *Journal of Public Policy*, 40, 1984, 19 ss.

replaced?) by the European regional institutions.

The complex, yet incomplete, nature of U.S. data privacy law has been often criticized by commentators[112] for preferring economic and securitarian interests over individual's freedoms[113].

It is a well-known fact that the federal agencies are very committed to data-trawling activities, collecting all kind of information regardless of their relation with the purpose of such a measure[114].

The U.S. data privacy legal framework consists of a three-tiles mosaic including: statutory instruments, law-cases and, to a lesser extent, constitutional rights[115]. The very first legislation addressing information stored in computerized databases was the 1970 Fair Credit Reporting Act (FCRA). FCRA is the archetype for every subsequent U.S. data-privacy legislation. It establishes mandatory notice and consent to and by citizens for specific data record. Additionally, it sets an administrative procedure for individuals redress by a specific agency. Finally, it covers the interests of law enforcement and national security, by defining the criteria under which those protected data are accessible[116].

In 1974 another milestone was set. The U.S. Department of Health, Education and Welfare (HEW) published a report titled "Computers and the Rights of Citizens". The paper recommended adopting a Code of Fair Information Practices (FIPs), all data users would be required to adhere to[117]. The five fair practices are: to forbid the creation of personal information secret databases; to provide to the individual mandatory access to his own data; to prohibit the use of personal data for purposes different from those for which they had been collected without a specific consent; to provide a way for the data subject to correct information about himself; to impose a duty of care to protect personal data from abuse or misuse[118].

The importance of the FIPs cannot be understated as it affected every other da-

---

[112] F. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, cit., 2007.

[113] However this did not prevent the Judiciary from swinging between libertarian orientations in *Klayman v. Obama*, Civ. Us. Colu. Dist. Court, no.13-0851 (2013) and more securitarian ones in *ACLU v. Clapper*, Us. NY South Dist. Court, no. 13 Civ. 3994 (2013). Not to mention, in *United States v. Jones*, 132 S. Ct. 945 (2012), five justices asked to re-think the Fourth Amendment application in light of the new technologies' expansion.

[114] J. Robinson, *The Snowden Disconnect: When the Ends Justify the Means*, in *SSRN*, 21 April 2014. However, this doesn't mean that there is no debate within the United States' academic community, nor that the Judiciary embraced the "security cause" blindly. See D.J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security,* in *Yale Un. Press*, 2011 and *ex plurimis* L.P. Vanoni, *Il Quarto emendamento della Costituzione americana tra terrorismo internazionale e datagate: Security v. Privacy*, in Federalismi.it*,* 2015,

[115] P.P. Swire-K. Ahmad, *U.S. Private-Sector Privacy*, Portsmouth, 2012.

[116] These can range from the probable cause to the *subpoena* or a simple request from an agency administrator.

[117] R. Gellman, *Willis Ware's Lasting Contribution to Privacy: Fair Information Practices*, in *IEEE Security and Privacy*, 12, 2014, 51-54; J. Waldo-H. Lin-L.I. Millett, *Engaging Privacy and Information Technology in a Digital Age*, Washington D.C., 2007.

[118] Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, Washington D.C., 1973, xx-xxi.

ta-legislation throughout the world[119]. Indeed, the five practices have been mirrored in 1980 OECD data privacy guidelines[120] and 1981 Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[121]. Afterwards, both these documents have impacted the primary EU legal instrument on Data protection: Directive 95/46/EC[122]. Due to their foresight, FIPs have been remarkably durable, and it took many decades to eventually adopt newer means of protection.

Later on, Washington embodied the FIPs in the 1974 Privacy Act (PA). However, here came the first obstacle to the U.S. leadership in privacy protection. The PA applied only to federal agency databases. This arguable choice was taken due to the concerns that the inclusion of the private actors would have stifled trade and burdened businesses[123]. Despite Warren and Brandeis' early attempt to establish individual rights primacy over economic interests, the PA handed a major victory over the said interests, in favour of the commercial lobbies[124].

However, it must be noted that this legislation has been adopted prior to the current mass digitalization, when the use of data storing devices was still circumscribed to few realities and propagating slowly, thus allowing the Congress to pinpoint specific categories of data singularly as they emerged.

Nowadays the U.S. are still lacking a general privacy regulation, yet they have adopted a discreet amount of Acts governing specific data traffics. Accordingly, privacy legislation was shaped like a fishnet, gradually reducing the meshes size with every new act. After the FCRA and PA came the Family Educational Rights and Privacy Protection Act of 1974 (FERPPA)[125]. However, with every new statue another problem arose: the absence of a common Supervisor Authority[126]. In fact, depending on the field (economy, healthcare, welfare etc.) every set of data has different requirements for appealing to the respective Authority, an arguably effective design. Eventually, the lack of

---

[119] M. Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, in *Stanford Technology Law Review*, 1, 2001, 44-47.

[120] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2013, available at www.oecd.org.

[121] COE, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981.

[122] D.J. Solove-P.M. Schwartz, *Information Privacy Law*, New York, 2011, 37-40; N.L. Richards, *Why Data Privacy Is (Mostly) Constitutional*, in *William & Mary Law Review*, 56, 1510. Joel Reidenberg suggested reducing the FIPs to only four principles: standards for data quality (forbidding any use different from the purpose according to which they have been acquired); transparency or openness of processing; special protection for sensitive data; standards of enforcements to ensure compliance, J. Reidenberg, *Setting Standards for Fair Information Practices in the U.S. Private Sector*, in *Iowa Law Review*, 80, 1995, 497 and 514-516; P.P. Swire-K. Ahmad, *op. cit.*

[123] P.M. Regan, *Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations*, in *Journal of Public Policy*, 4, 1984.

[124] *Ibid.*, 19-34.

[125] The 1974 FERPA addressed the privacy of student education records, assigning its oversight to the Department of Education. To access those data its required a judicial order or a lawful subpoena, E. Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment and Statutory Law Enforcement Exceptions*, in *Michigan Law Review*, 111, 2013 and 20 USC, 1232g (2012).

[126] Health Insurance Portability and Accountability Act (HIPAA) with Department of Health oversight, FERPA to the Department of Education, FCRA the Federal Trade Commission etc.

a comprehensive data privacy legislation, together with the U.S. judicial review system, made the Fourth Amendment the fulcrum of privacy protection[127]. However, courts interpretations often lacked vision, whenever the personal information disclosed had been processed in digital form, collected outside the "home-walls" or shared with a third party[128].

Therefore, it is not surprising that the Financial Privacy Act of 1978 (FPA) was specifically passed to counter some SCUS strict decisions, so to protect a specific set of data, the bank accounts, maintained by a third party[129]. The same applies to the emergence of cable TV industry, which promoted the 1984 Cable Communication Policy Act (CCPA), the video rental business the 1988 Video Privacy Protection Act (VPPA)[130], the rise of financial institutes other than banks led to the 1999 Gramm-Leach-Bliley Act (GLBA)[131]. Finally, the increasing number of genetic studies on hereditary diseases resulted in the adoption of 2008 Genetic Information Non-discrimination Act[132] adoption, in order to defend such sensitive data from the bottomless appetites of the Health Insurances. Nonetheless, no matter how thin the mesh is, there is no possible way for this method to effectively cover the continuously increasing amount of data exchanged.

However, the US legal system is not only composed by federal legislation. Indeed, many of the 50 States have passed regulations mandating a stronger protection of personal information than the federal government requires[133]. Ten of them even explicitly mention privacy in their own constitutions, 47 out of 50 have data privacy legislation, California has even banned the "stingrays" surveillance technology[134].

Additionally, in the last 15 years the Federal Trade Commission (FTC) has started

---

127 Even though it does not explicitly mention it. See R.J. Peltz-Steele, *The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation*, in *Journal of Internet Law*, 19, 2015, 17.

128 *US v. Miller,* see also S. Pell-C. Soghoian, *A Lot More than Pen Register, and Less than a Wiretap*, in *Yale Journal of Law and Technology*, 16, 2015, 134 ss. However, a "narrow opening" has been recently made by the Supreme Court in *Carpenter v. US* Sup. Court, no. 585 (2018). The Court ruled (5 Justices out of 9) that access to a person's historical cell-site records—or at least seven days or more of cell site records—is a Fourth Amendment search, for it breaches the person's «legitimate expectation of privacy in the record of his physical movements» and thus their access requires a warrant. Even though the ruling doesn't overrule the third party doctrine, it clearly shows a certain awareness of its inadequacy.

129 Financial Privacy Act of 1978 data are controlled by the Department of Treasure, even though the Act have been amended many times in order to enable easier access to financial information and promote reporting to the authorities as Treasury Financial Crimes Enforcement Network. The SCUS decision leading to its adoption is *Fisher v. United States*, 425 U.S. 391 (1976).

130 In contrast to SCUS decisions to allow rental records public disclosure. Actually there is an attempt to extend it also to the Netflix views activity, see J. Halpert-S. White, *Congress Makes Compliance with Confusing Video Privacy Protection Act Easier*, in Dlapiper.com, 9 January 2013.

131 Banning pretexting, a form of social engineering to gain access to private financial data secretly and requiring financial institutes to collaborate with the federal agencies.

132 There are many other sectors singularly protected as the telephone records by the 2006 Telephone Records and Privacy Protection Act., personal health information by the 1996 Health Insurance Portability and Accountability Act (HIPAA), 1994 Driver's privacy Protection Act, 1998 Children's Online Protection Act etc.

133 National Conference of State Legislature, *Privacy Protection in State Constitutions*.

134 C. Farivar, *California Cops, Want to Use Stingray? Get a Warrant, Governor Says*, in ArsTechnica.com, 10 September 2015.

to sanction companies for exposing the data they collected from consumers to the threat of breach, thus shaping data privacy in commercial practices[135]. The Commission primarily based its authority on an extensive interpretation of the FTC Act, which prohibits «unfair practices in or affecting commerce»[136]. However, in 2014 the *FTC v. Wyndham Worldwide Corp.*[137] set in law-case the agency's authority over data security. The agency, invested of such an authority, developed a doctrine of harm potentially troublesome[138], causing only actual financial losses related directly to the disclosure to be persecuted. Nonetheless, the U.S. courts had been wavering so far, between recognizing or not illegitimate personal data retention or disclosure by a commercial entity as wrong *per se*.

In conclusion, the U.S. privacy regime looks quite inefficient, as it is characterized by a high fragmentation. A multi-layer legal system including a federal statutory "fishnet", many Supervisory Authorities, States' constitutions or specific data legislation and heterogeneous judicial interpretation[139]. It is not surprising that such a complex system has difficulties in keeping the pace with the digital age.

However, besides the structural difficulties, the major challenge the U.S. are now facing are their security measures. In 2013 Snowden's revelations, also known as *Datagate*, disclosed the systematic system of surveillance by the National Security Agency (NSA) of both American and foreign citizens whose data were collected in American servers. The International scandal highlighted the US Government choice to provide national security interests the upper hand over privacy[140], resulting in the CJEU repeal of the EU Commission Decision 2000/520/EC regarding the data transmission from EU to the USA. As a consequence, the *Datagate* sealed the end of the American leadership in data protection definitely, thus handing over the "baton" to the EU.

---

[135] Among many see *FTC v. Eli Lilly*, C-4047 (2002). E. Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, cit., 485 ss.; A. Serwin, *The FTC v. Wyndham Reexamined — A True Test of the Contours of Unfairness*, in *The Lares Institute Blog*, 2015; G. Stevens, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, in *Fas.org*, 11 September 2014.

[136] 15 U.S.C. § 45.

[137] *FTC v. Wyndham Worldwide Corp*. 799 F.3d 236 (3d Cir. 2015) Wyndham Worldwide used a property management system that processed consumer information, including names, addresses, contact information, and credit card information. In 2008 and 2009, Wyndham's network and property management systems were hacked three times. Hackers allegedly accessed unencrypted information for over 619,000 accounts, resulting in approximately $10.6 million in fraud loss.

[138] A. Serwin, *The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices*, in *San Diego Law Review*, 48, 2011, 809 ss.

[139] D. Ombres, *NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform*, in *Seton Hall Legis Journal*, 39, 2015, 27 ss.; D. Lyon, *The Snowden Stakes: Challenges for Understanding Surveillance Today*, in *Surveillance and Society*, 13, 2015, 139 ss. G. Gutierrez, *Imbalance of Security and Privacy: What the Snowden Revelations Contribute to the Data Mining Debate*, in *Intellectual Property Law Bulletin*, 19, 2014, 161 ss.

[140] D. Ombres, *NSA Domestic Surveillance from the Patriot Act to the Freedom Act: The Underlying History, Constitutional Basis, and the Efforts at Reform*, in *Seton Hall Legis Journal*, 39, 2015, 27 ss.

2.2. EU Data privacy. You can teach an old Continent new tricks

Due to its founding Treaties, the EU has been quite prone to offer an appropriate level of protection to both private life and data privacy. Therefore, when the former legal framework (Directives 95/46/EC and 2006/24/EC) has been overtaken by the rapid technological developments, the CJEU decisions acted as first "line of defence", only to be later seamlessly transferred into the new Regulation (EU) 2016/679.

Directive 95/46/EC, adopted on the basis of Art. 95 TEC, established the core framework of the personal data protection. In addition, it also urged each Member-States to make Independent Supervisory Authorities entitled to control the data flows. The directive has been a flexible regulation both formally and substantially, due to the implementation and interpretation of its regulatory content. Nonetheless, its pliancy has been the major cause of its demise in 2018 May.

Clearly inspired by the CoE Convention no. 108[141], the directive has been a milestone in the regulation of personal data protection in the EU[142]. Moreover, the directive provisions were sufficiently detailed to be considered self-executive, hence it could be directly invoked by the European citizens against the Member-State not complying with it[143]. However, the regulation was adopted (as its inspiring legislation[144]) at the dawn of digital Age, long before it reached the actual peak. The regulation merely set down the general rules for the treatment, detection and update of personal data. Nonetheless it left ample room for national legislation to determine the processing lawfulness conditions. The directive was meant to harmonize the previous fragmented regime, which was hindering data flows within the internal market, thus hampering the European commercial activities[145]. Therefore, the motive behind the directive was undoubtedly economic. Moreover, the 1995 regulation urged each Member-State to establish a Privacy Supervisory Authority. Additionally, it defined the legal meaning of "personal data", "processing of personal data", "personal data filing system", "controller", "processor", "third party", "recipient", and "the data subject's consent", which are now

[141] The phenomenon of the "duplication" among CoE Convention and EU legislation is well known, for analysis see A. Von Bogdandy, *Pluralism, Direct Effect, and the Ultimate Say: On the Relationship Between International and Domestic Constitutional Law*, in *International Journal of Constitutional Law*, 6, 2008, 397 ss.; W. Burke-White, *International Legal Pluralism*, in *Penn Law Legal Scholarship Repository*, in *Michigan Journal of International Law*, 25, 2005, 963 ss.; V. Salvatore, *Nuove norme in materia di trattamento automatizzato dei dati personali*, in *Rivista internazionale dei diritti dell'uomo*, 1993, 73-79.

[142] A. Pisapia, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in Federalismi.it, 3, 2018, 15.

[143] B. De Witte, T*he Continuous Significance of Van Gend en Loos*, in M. Poiares Maduro-L. Azoulai (eds.), *The Past and the Future of Eu Law*, Oxford, 2010, 11 ss.; H. Labayle, *Refonder l'espace de liberté, de sécurité et de justice à la lumière de l'arrêt Van Gend en Loos?*, in *50th anniversary of the judgment Van Genden Loos 1963–2013*; K. Lenaerts-T. Corthaut, *Of Birds and Hedges: The Role of Primacy in Invoking Norms of EU Law*, in *European Law Review*, 31, 2006, 287 ss.; A. Nollkaemper, *The Duality of Direct Effect of International Law*, in *European Journal of International Law*, 25, 2014, 105 ss.; J.H.H. Weiler, Van Gend en Loos*: The Individual as Subject and Object and the Dilemma of European Legitimacy*, in *International Journal of Constitutional Law*, 12, 2014, 96 ss.

[144] FIPs, ECHR, Coe Convention no. 108, *etc.*

[145] A. Pisapia, *op. cit.*, 16.

used worldwide[146].

Directive 95/46/EC sets many new data treatment criteria. The general rule of unambiguous consent contained in Art. 7, establishes expressly when data processed must be qualified as sensitive pursuant to Art. 8. In addition, Artt. 10 and 11[147] enforce the right to be informed, which should be read in conjunction with Art. 12 by stating that being informed to one's own data processing/collection is indispensable to properly exert the right to access or, if necessary, to modify, block or delete data. However, Art. 25 is by far the most interesting, as it tried to address the supranational dimension of data flows, requiring «an adequate level of protection»[148] by every country to which European citizens data were transferred to.

Despite its unquestionable merits, Directive 95/46/EC did not sufficiently prevent the national proliferation of data-processing regulations related to new technologies or anti-terrorism[149].

In 2008 the situation started changing. In *Satamedia*[150] Advocate General Kakott deemed necessary to align Art. 9 of the directive with Artt. 7 and 8 ECHR as interpreted by the Strasburg Court[151].

With the Lisbon Treaty enforcement, it became necessary and indefectible to introduce a common binding regulation to assure all European citizens a univocal level of protection for privacy. In the meanwhile, the responsibility to protect European citizens' rights from the new threats was entrusted to the CJEU. In the decision C-553/07 of 7 May 2009, regarding the access to personal data, the Court sanctioned the asymmetry between the duration and the exercise of people's right of access to their own data and the obligation entrusted to the controller to retain them for an extended period of time. In the joined Cases C-293/12 and C-594/12, the so-called 2014 "*data retention*" ruling declared invalid Directive 2006/24/EC for not being proportionate. The directive allowed the Member States, within the fight against terrorism and organized crime, to indiscriminately collect ad retain citizens' personal data for a period ranging from 6 to 24 months. Lastly, the decision of the Court of Justice, dated 13 May 2014 (the so-called "*Google case*"), which extended a case regarding the processing of personal data to the results of the search engines and provided an "authentic interpretation" of the rights afforded by Directive 95/46/EC, widened the rights of the concerned parties regarding the availability of their data, thus recognizing a true "right to be forgotten". All these fruits (*Digital Rights Ireland*, *Schrems*, *Google, Tele2 Sverige* etc.) will be later reaped

146 Art. 2, Directive 95/46/EC.

147 Art. 11, Directive 95/46/EC. If the data have not been given by directly by the data subject, the controller or his representative must provide him with at least the following information, «(a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) any further information such as — the categories of data concerned, — the recipients or categories of recipients, — the existence of the right of access to and the right to rectify the data concerning him».

148 Art. 25, Directive 95/46/EC.

149 Recital 9; see also D. Erdos, *European Data Protection Regulation and the New Media Internet: Mind the Implementation Gaps*, in *Journal of Law and Society*, 43, 2016.

150 CJEU, C-73/07, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* (2008).

151 Opinion of the AG, 8 May 2008, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy und Satamedia Oy*, § 37

by the incoming legislation.

As soon as the EU Commission acknowledged the fact that the Technological revolution rapidity had radically altered the European citizens' rights, it announced a new common legislation project addressing the new forms of data privacy[152]. Moreover, after the Lisbon Treaty, the Charter of Fundamental Rights of the European Union (CFREU) has been added to the European primary legislation.

The Charter at Art. 8[153] and the TFEU at Art. 16[154] explicitly mention data protection as fundamental right, thus separating it from "traditional" privacy. Therefore, a regulation appeared necessary to ensure within the European Union European the same level of protection and enjoyment of such fundamental right[155].

In 2012 the Commission submitted two legal instruments: a European regulation project (Regulation (EU) 2016/679) intended to replace Directive 95/46/EC and a new directive replacing Framework Decision 977/2008/EC (regarding data processing within the fight against crime and terrorism)[156].

As well known, Regulations are measures of general scope, binding in their entirety and directly applicable by the Member-State Authorities, thus further guaranteeing legislative harmonization within the single market[157]. The main difference from previous legislation is that Regulation (EU) 2016/679 does not pursue anymore primarily economic interests[158]. The Regulation aims to guarantee the same level of data privacy protection to each European citizen, regardless of his/her nationality or place of residence (recital 10). It opens a new era of commitment to data protection establishing a new set of basic guarantees and harsher sanctions for the offenders[159]. The Regulation

[152] Commission Communication Com (2010) 609.

[153] Art. 8 CFREU: «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».

[154] H. Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Art. 16 TFEU*, New York, 2016.

[155] F. Donati, *Art. 8. Protezione dei dati di carattere personale*, in R. Bifulco-M. Cartabia-A. Celotto, *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Bologna, 2001, 83 ss.

[156] Com (2012) 9. Notably, during our never-ending "war on terror" security measures were one of the main obstacle to a sufficient harmonization of European data protection legislations. Nevertheless, it can be noted how the EU is steadily tightening its grip on data processing, substituting a directive with a regulation and a framework decision with directive. Therefore, the EU has considered, according to the subsidiarity and proportionality principles, these means more suited to achieving its objective. Regarding the EU legislative range see: L. Daniele, *Diritto dell'Unione Europea*, Milano, 2014; E. Cannizzaro, *Il diritto dell'integrazione europea*, Torino, 2015; G. Strozzi-R. Mastroianni, *Diritto dell'Unione europea, Parte generale*, Torino, 2013; G. Tesauro, *Il diritto dell'Unione Europea*, Padova, 2015.

[157] C. Blumann-L. Dubois, *Droit institutionnel de l'Union européenne*, Paris, 2013; M. Dony, *Droit de de l'Union européenne*, Brussels, 2014; G. Gaia-A. Adinolfi, *Introduzione al diritto dell'Unione europea*, Bari, 2014; T. Hartley, *The foundation of European Union Law*, Oxford, 2014; A. Rosas-L. Armati, *Eu Constitutional Law*, Oxford, 2012.

[158] For an analysis of how the CJEU role has changed after the enforcement of the Lisbon Treaty see. G.F. Aiello, *La protezione dei dati personali dopo il Trattato di Lisbona*, in *Osservatorio del dir. civ. e comm.*, 2, 2015, 431; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

[159] G. Finocchiaro (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*,

aims to ensure each European citizen the same level of data privacy, regardless of their nationality or place of residence (recital 10). Not surprisingly, it does not affect activities falling outside the scopes of European Law, as secondary legislation cannot amend the competence boundaries set by the treaties[160]. For instance, the Regulation itself excludes explicitly from its implementation the treatments performed for security purpose[161]. Nevertheless, it also repeals the aforementioned Framework Decision 2008/977/GAI, regulating judiciary and criminal cooperation of the Member States.

Regulation (EU) 2016/679 acknowledges that in a *data intensive* context the very nature of personal data has changed. Nowadays it is possible to obtain highly confidential information simply by cross-checking apparently harmless data, neither considered sensitive, nor personal by EU or national legislations. This phenomenon has been facilitated by the Big Data[162], which continuously gather and store information, only to have them analysed by Data brokers[163]. Therefore, the Regulation has widened the conception of personal data including any information relating to an identified or identifiable natural person, thus considering every information which may lead to a person identification trough cross-checking[164]. Additionally, it demands the data subject to be informed with regard to his own data automatic processing[165]. Moreover, he is granted a right to oppose such a treatment along with a "right to explanation" of its benefits and consequences[166].

However, the main change lies in the data controller accountability for the data treatment. Data controllers are now demanded to adopt — with the boundaries of proportionality and "affordability" — any mean the state of the art offers (privacy by design, security measures etc.) in order to protect the processed data[167]. The compliance with

Bologna, 2017.

160 With regard to the competence regulation within the EU see v. F. Bassanini-G. Tiberi (a cura di), *Le nuove istituzioni europee. Commento al Trattato di Lisbona*, Bologna, 2010, 154 ss.; P. Craig, *Competence and Member States Autonomy: Causality, Consequences and Legitimacy*, in H.W. Micklitz-B. De Witte (eds.), *The European Court of Justice and the Autonomy of Member States*, Cambridge-Antwerp-Portland, 2012, 11 ss.; R. Mastroianni, *Le competenze dell'Unione*, in G. Morbidelli-F. Donati (a cura di), *Una Costituzione per l'Unione europea*, Torino, 2006, 131 ss.

161 R. Baratta, *Le competenze interne dell'Unione tra evoluzione e principio di reversibilità*, in *Il Diritto dell'Unione Europea,* 15, 2010, 517 ss.; E. Cannizzaro, *Sovranità degli Stati ed esercizio di competenze dell'Unione Europea*, in *Il Diritto dell'Unione Europea,* 2, 2000, 241 ss.; V.M. Sbrescia, *Le competenze dell'Unione europea nel Trattato di Lisbona*, Napoli, 2008, 343 ss.; M. Scudiero (a cura di), *Il diritto costituzionale comune europeo. Principi e diritti fondamentali*, Napoli, 2002, 329 ss.

162 G. D'Acquisto-M. Naldi, *Big data e privacy by design*, Torino, 2017, 59 ss.

163 S. Calzolaio, Privacy by design. *Principi, dinamiche, ambizioni del nuovo Reg. Ue 2016/679*, in *Federalismi. it,* 24, 2017, 6; *Privacy by Design in Big Data. An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, European Union Agency for network and information security, December 2015.

164 G. Giannone Codiglione, Risk-based approach *e trattamento dei dati personali*, in S.Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della* privacy, Padova, 2016, 64; S. Calzolaio, *op. cit.,* 12.

165 Art. 22, Regulation (EU) 2016/679.

166 Artt. 13, 14 and 15, Regulation (EU) 2016/679; see also B. Goodman-S. Flaxman, *European Union Regulations on Algorithmic Decision-making and a 'Right to Explanation'*, in *AI Magazine,* 3, 2017; S. Wachter-B. Mittelstadt-L. Floridi, *Why a Right to Explanation of Automated Decision - Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 7, 2017.

167 Art. 24(2), Regulation (EU) 2016/679.

these requirements has to be proved through a certification released pursuant to Art. 42 of the Regulation. Another feature is that, whenever the data controller is a public authority or body[168] or the controller is exerting large scale data monitoring and processing, the new Regulation requires them to designate a Data Protection Officer (DPO)[169]. The DPO new figure is responsible for ensuring the enforcement of the Regulation by the *data collector*, training its staff, promoting the adoption of "privacy by design and default" tools and acting as intermediary body between corporates or public bodies and the national Data Protection Authorities[170].
Finally, the Regulation, as its predecessor, takes on data flows supranational dimension. However, in order to grant an adequate protection, it requires foreign data collector its enforcement as *condicio sine qua non*, in order to access the European data market.
In conclusion, the Regulation has the ambitious merit to try to muzzle the economic and technological forces so to actually promote and strengthen the protection of data privacy, thus imposing a crucial paradigm shift.

3. New challenges and solutions

If data privacy has originated in the second half of the XX century, it is only recently that our society has massively digitalized. This is due to many factors, the main one being the market. If the first databases had been made by public or quasi-public agencies, nowadays data collection is made mainly by private companies.
At the dawn of new millennium privacy had to deal with the rise of the "*over the top*" data collectors as Facebook, Google, Twitter, etc. Indeed, social networks and search engines are storing an amount and variety of information once unimaginable. Appropriately questioned, even the most harmless data, when gathered, can reveal sensitive information about their data subject. This opportunity stimulated market, leading to the creation of a new business activity: Data-broking. Moreover, such an information-estate ended up attracting the governments, that are increasingly looking for information suitable to anticipate the potential threats to their security as the war on terror drags.

3.1 National security and privacy, an obnoxious relationship

Nowadays it is undeniable that one of the main threats to privacy comes from the subject responsible for its protection: the State.
In Western democracies the adoption of emergency regimes has always been a physiological reaction to internal or external threats to internal peace and security. Despite George W Bush and François Hollande enthusiastic declarations of war on terror or

[168] Except for the courts acting in their judicial capacity.

[169] Art. 37(1), Regulation (EU) 2016/679.

[170] Artt. 13 and 14, Regulation (EU) 2016/679.

ISIS, eminent scholars have already pointed out how strictly speaking, in the absence of a sovereign country, the current conflict looks more likely an international police operation than a war[171]. Indeed, Terrorism stands on the crossroad between war and crime. In fact, despite its perpetrators being foreign or radicalized citizens, their attacks have shown to be as deadly as actual warfare[172]. This very indeterminacy compelled Western democracies to adopt anticipatory and covert measures based on the sheer suspect[173]. On one hand, we have assisted to the enhancement of administrative police measures (either outlined in emergency states or ordinary statues) limiting traditional freedoms[174]. On the other, every country is altering the balance of powers in favour of the Executives, which are considered more suited to face such an emergency[175].

In spite of the temporary nature of the measures, emergency legislation has proven to be a tool with an extraordinary longevity. This has been particularly true for the United States[176], followed by the UK[177], France[178] and many other European countries[179]. The necessity to prevent the attacks requires to gather as much information as possible about the targets, organizers etc., thus addressing more detailed and wide forms of control over the population. It explains why information flows have become the actual battlefield of this asymmetric war, and data gathering has primary role in it[180].

The technologic revolution has offered to the States countless new surveillance means exploiting the society digitalization. It is fair to say that the access to personal information has never been so easy.

The first measures restricting privacy have been adopted in the US, starting with the infamous 2001 USA Patriot Act[181]. As revealed by Edward Snowden during the *Datagate*, the US federal security agencies were responsible for massively collecting personal information from individuals all over the world. This major infringement had been

---

171 G. De Vergottini, *La "guerra" contro un nemico indeterminato*, in *Forum di Quaderni Costituzionali,* 5 October 2001; A. Vedaschi, *À la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Torino, 551.

172 W. Laqueur, *The Age of Terrorism*, Boston, 1987, 7; v. C. Walter, *Defining Terrorism in National and International Law*, in C. Walter (ed.), *Terrorism as Challenge for National and International Law: Security versus Liberty?*, Berlin, 2004, 23-25 and T. Becker, *Terrorism and the State, Rethinking the Rules of State Responsibility*, Oxford-Portland, 2006, 83 ss.

173 S. Gambino-A. Scerbo, *Diritti fondamentali ed emergenza nel costituzionalismo contemporaneo. Un'analisi comparata*, in *Diritto Pubblico Comparato ed Europeo*, 4, 2009, 1.

174 A. Vedaschi, *op. cit.*, 513 ss.

175 E. Posner-A. Vermeule, *Terror in the Balance: Security, Liberty and the Courts*, Oxford, 2007.

176 C. Bassu, *Terrorismo e costituzionalismo. Percorsi comparati*, Torino, 2010; F. Lanchester, *Gli Stati Uniti e l'11 settembre 2001*, in *Rivista AIC*; P. Bonetti, *Terrorismo, emergenza e costituzioni democratiche*, Bologna, 2006; G. de Vergottini, *Guerra e costituzione. Nuovi conflitti sfide alla democrazia*, Bologna, 2004.

177 2016 Investigatory Powers Act.

178 État d'urgence, Law 20 November 2015, no. 1501.

179 In Italy see Law Decree 18 February 2015, no. 7, granting police officers access to personal information on the ground of a simple regulatory measure.

180 S.W. Brenner, *Cybercrime, cyberterrorism and cyberwarfare*, in *Revue internationale de droit penal*, 77, 2007, 453 ss.; F.R. Fulvi, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *Diritto penale e processo*, 5, 2009, 639 ss.; C. Sarzana di Sant'Ippolito, *Sicurezza informatica e lotta alla cybercriminalità: confusione di competenze e sovrapposizione di iniziative amministrative e legislative*, in *Diritto dell'Internet*, 5, 2005, 437 ss.

181 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* Act of 2001, Public Law no. 107-56.

possible due to the fact that most ICT and Big Data servers are located on the American soil. It resulted in their inability to refuse security agencies access to their database. This is not an isolated case, as many European countries have only recently decided to adopt more far-reaching security measures, trying to address both the interest in the use of new surveillance means and the interest in their limitation.

The relevance of data analysis in counter-terrorism operations has required to redraw the line between security and privacy. Given the security contentious nature[182], most commentators have agreed on its basic function as a limit to the rights, rather than an autonomous right[183]. Therefore, when analysing the constitutionality of security measures, it is more appropriate to evaluate them in terms of proportionality between extent and purpose (*quantum* and *quomodo*), rather than balance between rights[184]. It is not surprising that during the last decades both Constitutional and International courts have tried to shape the relationship between the new-born data privacy and counter-terrorist legislation.

In France, the reform of the *État d'urgence*[185] has led to rise three *questions prioritaires de constitutionnalité* before the Conseil Constitutionnel[186]. Nonetheless, only QPC no. 2016-536 was (partially) upheld. The Conseil found *loi* no. 55-385 new Art. 11 unconstitutional, as it enabled police officers to collect all the data stored in the digital devices collected during the course of a home search with no seizure warrant issued by a judge. Moreover, Art. 11 enabled the proceeding authority to download data regardless of their correlation with the offence, without setting any criteria as the duration of their retention or any security standard[187].

In Germany, the Bundesverfassungsgericht has decided twice over the proportionality of "digital" security measures. In 2008 it declared, for the first time, unconstitutional a statue enabling remote access to private IT systems, thus recognizing the primacy of

[182] Strictly speaking we should speak of proportionality of the security measure, rather than balance between privacy and security. For a further analysis of security nature as a right or interest see A. Pace, *Libertà e sicurezza. Cinquant'anni dopo*, in A. Torre (a cura di), *Costituzioni e sicurezza dello Stato*, Rimini, 2014, 547 ss.; M. Dogliani, *Il volto costituzionale della sicurezza*, in G. Cocco (a cura di), *I diversi volti della sicurezza*, Milano, 2012, 1 ss.; P. Ridola, *Libertà e diritti nello sviluppo del costituzionalismo*, in P. Ridola-R. Nania (a cura di), *I diritti costituzionali*, Torino, 2006; *contra* G. Cerrina Feroni-G. Morbidelli, *La sicurezza: un valore superprimario*, in *Percorsi costituzionali*, 1, 2008 and T.E. Frosini, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali,* 2006.

[183] A. Cerri, *Diritto alla riservatezza e videosorveglianza*, in M. Manetti-R. Borrello (a cura di), *Videosorveglianza e Privacy*, Firenze, 2010, 18.

[184] A. Ruotolo, *Costituzione e sicurezza tra diritto e società*, in A. Torre, *Costituzioni e sicurezza dello Stato*, Rimini, 2014, 588. As aforementioned, the European legal systems recognize both privacy and data protection as a fundamental rights. When not explicitly mentioned, as in the Italian constitution, it is often associated to the personal and moral freedoms. L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Napoli, 2016, 14. Not to mention the many international charters as the 1981 COE Convention no. 108, Artt. 7 and 8 ECHR, Art. 16 TFEU and Art. 8 Treaty of Nice.

[185] By *Loi n. 2015-1501 du 20 novembre 2015.*

[186] The Conseil had already harmonized security measure and individual rights, a recurrent issue in its jurisprudence. See Decisions nn. 85-187 DC e 2003-467 DC.

[187] Such as irrelevant personal information or even related to uninvolved third parties. For a comment see S. Scagliarini, *La* privacy *al tempo dell'*état d'urgence*: il Conseil constitutionnel sentenzia correttamente*, in *ConsultaOnline*, 1, 2016, 191.

privacy over investigation requirements[188]. On 20th April 2016. The Court questioned then proportionality of the Bundeskriminalamtgsetz (BKAG), which similarly allowed access to personal data via remote. Notably, the Court considered the Trojans unable to grant a meaningful privacy protection, as the collected data were immediately transferred to the federal police office, bypassing the *Bundesbeauftragte für den Datenschutz*[189].
With regard to the Council of Europe, it has been already stated that the ECHR catalogue of rights includes privacy (Art. 8). After the terrorist emergency, the Court of Strasburg has ruled many times over the restriction of fundamental rights for security purpose[190]. The case *Szabò and Vissy v. Hungary* is the latest in a long series of rulings. One of its last decision has been delivered in a case concerning two Hungarian lawyers, who challenged before the Constitutional Court of Hungary the 2011 Police Act, according to which police officers are empowered to conduct a wide range of secret surveillance activities and even seizure on the ground of a simple Secretary of Justice authorization[191]. Moreover, all operations carried out by the police didn't require an assessment of strict necessity nor judicial oversight[192].
Within the European legal context, it must be noted that the path opened by the European Court of Human Rights has influenced the Court of Justice of the European Union. Even though the Court of Luxembourg has become a full-fledged "judge of the rights" only after the Treaty of Lisbon[193].
In the last decade the CJEU has dealt with issues connected to data privacy and the proportionality of its limitation.
In *Digital Right Ireland* (DRI)[194], the Court declared invalid Directive 2006/24/EC of the European Parliament and Council — which modified Directive 2002/58/EC — regulating the retention of data generated or processed by ICT service providers. The directive ensured Member-States greater investigation powers in areas relevant to counter terrorism and every that crime national legislations recognized as a serious offence.

---

188 BVErfG 27 February 2008, 1 BVR 370/97. The measure allowed to inspect the devices content and browsing history.

189 BVErfG 20th April 2016, 1 BVR 966/09. For a comment see L. Giordano-A. Venegoni, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in www.penalecontemporaneo.it, 8 May 2016.

190 There is a large body of case law focusing on the relationship between privacy and security-investigations needs, see ECtHR, *Malone v. UK,* app. 8691/79 (1984); *Kruslin v. France,* app. 11801/85 (1990); *Rotaru v. Romania,* app. 28341/95 (2000); *Taylor-Sabori v. UK,* app. 47114/99 (2002); *Peck v. UK,* app. 44647/98 (2003); *Perry v. UK,* app. 63737/00 (2003); *Matheron v. France,* app. 57752/00 (2005); *Vetter v. France,* app. 59842/00 (2005); *Copland v. United Kingdom,* app. 62617/00 (2007); *K.U. v. Finland,* app. 2872/02 (2008); *S. and Marper v. UK,* apps. 30562/04 and 30566/04 (2008); *M.K. v. France,* app. 19522/09 (2013).

191 Through secret recording of conversations, opening of letters and parcels, and checking and recording the contents of electronic communications, §§ 6-16.

192 § 89.

193 Thereafter, the EU Charter of Human Rights acquired a legally binding character through Art. 6(1) TEU, which gives the Charter the same legal value as the funding Treaties.

194 DRI reunited two preliminary rulings submitted by the High Court of Ireland and the Austrian *Verfassungsgerichthof*. *Digital Rights Ireland Ltd* (C-293/12), *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl et a.* (C-594/12), see S. Bonfiglio, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Democrazia e sicurezza*, 3, 2014.

Firstly, Directive 2006/24 allowed the indiscriminate collection and retention of a vast amount of personal information, regardless of their correlation with the prosecuted offences or of concerned people profiles[195]. Moreover, Art. 4 of the directive did not include «substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use»[196]. It entitled Member State to establish the procedures and conditions to access the retained data, without setting any guideline or fundamental criteria to be respected[197]. Finally, Art. 6 required that data to be retained from a minimum of 6 months to a maximum of 24 regardless of their usefulness to the investigation[198].

The Court subjected such measures to a strict proportionality test, which they didn't pass. The decision constitutes an important precedent because it is the first time a CJEU ruling has entirely repealed a secondary legislation due to its incompatibility with the Treaty of Nice, notably Artt. 7 and 8.

Another important CJEU ruling is the case *Schrems* or *Facebook*[199]. The Court invalidated the European Commission Decision 2000/520, authorizing an international treaty with the US, enabled personal data transfer of European citizens towards the other side of the Atlantic, this practice is also known as *Safe Harbor*[200]. Therefore, the Court dealt with two specific data protection issues: (again) the proportionality of security measure and the supranational dimension of data flows.

The concerned treaty allowed Big Data companies to have access to the European market and at the same time to maintain their main servers in the United States, as their privacy legislation met the European minimum standards. In 2013 the *Datagate* led an Austrian citizen Maximillian Schrems to question such a compliance to Art. 45 of Directive 95/46, as it became clear that the U.S. Patriot Act blatantly ensured national security a primacy unknown in Europe[201].

---

195 CJEU, C-293/12, *Digital Rights Ireland Ltd* (2014), § 59; *ex plurimis* see O. Pollicino, *Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it - focus TMT*, 3, 2014; Id., *La "transizione" dagli atomi ai bit nel reasoning delle Corti europee*, in *Ragion pratica*, 44, 2015, 53 ss.; Id., *Diritto all'oblio e conservazione di dati. la Corte di giustizia a piedi uniti: verso un "digital right to privacy"*, in *Giur. cost.*, 2014, 2949 ss. O. Pollicino-M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in G. Resta-V. Zeno Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dal "Safe Harbour principles" al "Privacy Shield"*, Roma, 2016, 73 ss.; L. Trucco, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali*, in *Giur. it.*, 8-9, 2014, 1850 ss.; M. Rubechi, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *Federalismi.it*, 23, 2016, 19.

196 *Digital Rights Ireland Ltd,* cit., § 60.

197 *Ibid.,* § 61-62.

198 *Ibid.,* § 63.

199 CJEU, C-362/14, *Maxmillian Schrems v. Data Protection Commissioner* (2015). For an in-depth analysis of the case see at least O. Pollicino-M. Bassini, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit.; S. Sileoni, *La tutela della riservatezza negli Stati Uniti e le nuove frontiere per la circolazione dei dati personali*, in *Quaderni costituzionali*, 4, 2015, 1027 ss.

200 The decision was taken according to Art. 25(6), Directive 95/46/EC.

201 For a comparative analysis of the issues raised by the personal data exchange between U.S. and E.U. see D. Cole-F. Fabbrini, *Bridging the transatlantic divide? The United States, the European Union, and the protection of privacy across borders*, in *International Journal of Constitutional Law*, 14, 2016, 220 ss.; I. Tourkochoriti, *The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation: In Search For Legal Protection Against Surveillance*, *Pennsylvania Journal of International Law*, 36, 2014, 459 ss;

The Court examined Decision 2000/520 and found the US privacy protection legislation severely inadequate and far from meeting the Directive 95/46 requirement, especially after its alignment with the Treaty of Nice[202]. As for *Digital Rights Ireland*, the Court established that any restriction to data privacy had strictly necessary, whilst the American legislation allowed a massive and indiscriminate collection information and loose access criteria for the security agencies.

As a consequence, the CJEU repealed the Decision 2000/520 entirely, urging the US to meet the European protection standards and both the US and EU to reconsider the terms of their data exchange. On one hand the ruling lead Washington to replace the infamous USA Patriot Act with the 2015 Freedom Act. On the other EU and US initialed the *Privacy Shield*, a new agreement providing the transfer of European citizens' data into servers located European soil.

This decision might have set in motion has a deep change in the US privacy policy. In 2015 Spring Microsoft Corporation initiated a legal proceeding against the US Department of Justice, denouncing the exponential increase in the number of requests for access to their databases. Afterwards, In 2016 July the US Court of Appeals declared inaccessible to the American agencies the data stored in servers situated outside the US territory even if owned by American companies[203].

The same reasoning lies behind the recent CJEU Opinion n. 1/15 of 26 July 2017, which prevented the conclusion of the agreement between the European Union and Canada on the transfer of Passenger Name Record (PNR). The Court observed that «Although the systematic transfer, retention and use of all passenger data are, in essence, permissible, several provisions of the draft agreement do not meet requirements stemming from the fundamental rights of the European Union»[204], thus forcing also the Canadian legislation to meet the standards set by EU law.

Finally, it must be noted that the path opened by the *Schrems* and *DRI* cases has been followed by two other important CJEU's rulings: the united cases C-203/15 and C-698/15, known as *Tele2 Sverige* and *Watson*[205]. The Luxembourg Court, asked by the Appeal Courts of Stockholm and England and Wales to verify their data-retention legislations compliance with EU law, seized the opportunity to further entrench its position on privacy and security.

The national legislation on one hand compelled the providers of electronic communication services to systematically retain all data related to said communications for a given amount of time, on the other it granted the national authorities an unlimited access to this information. The CJEU, not surprisingly though, detected the infringement of Directive 2002/58/EC — as interpreted according to Artt. 7 and 8 of the EU

L.P. Vanoni, *Balancing privacy and national security in the global digital era: a comparative perspective of EU and US constitutional systems*, in *Forum di Quaderni Costituzionali*, 14 June 2017.

202 Which after the Lisbon Treaty has become an actual European Constitution.

203 U.S. Court of Appeals, 2nd Cir, 14 July 2016 (Docket No. 14-2985).

204 CJEU, Press Release no. 84/17, Luxembourg, 2017, 1.

205 O. Pollicino-G.E. Vigevani, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza Tele2 Sverige della Corte di giustizia UE*, in *Forum di Quaderni Costituzionali*, 1, 2017; O. Pollicino-M. Bassini, *La Corte di Giustizia una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, January 2017.

Charter of Fundamental Rights —by the member States. Moreover, the Court established data-retention and access to be limited to what is strictly necessary to counter serious crimes and to be regulated by an independent authority. From now on, every legislation not meeting these requirements will not enjoy the discretionary margin set by Art. 15 of Directive 2002/58/EC. Has data-privacy finally managed to checkmate security on the European chessboard?

3.2. Data global Market, threat or treat?

The threat posed by the Digital age resides in technology's unbridled nature. A rapid and endless stream of trans-national[206] and anarchic[207] means, relentlessly eroding the "riverbanks" of Law. It is not surprising that the best attempt to regulate data privacy came from stakeholders on continental scale (U.S and E.U.) nor that the most proficient bodies have been the courts, capable to act swiftly, bypassing the statutory red-tape[208].

With regard to the supranational issue, it must be observed that the first attempt to deal with it came from the 1981 Convention no. 108 (also known as the Strasburg Convention) of the Council of Europe. It is important to note that the Convention in order to encompass as many counties as possible, can be ratified also by non-Member States, as Uruguay did in 2013. The same applies to the 2001 Convention 185/2001 (Budapest Convention)[209], regulating digital offences and particularly computer frauds and child pornography. Additionally, the Convention aims to project abroad the European human rights as well as the criteria of proportionality, necessity set in the ECtHR case law.

Even though international law offers the advantage to simultaneously address a multitude of Countries, the EU might have found a new mean.

The new Regulation (EU) 2016/679, in fact, is directly designed for all those national and foreign data collectors, who are compelled to meet the European standards required to access the European data market. Not only, the regulation takes into consideration the case *Google Spain* decision, and hence considers the data retainer responsible for the consequences of the information treatment and even for their databases breaching.

---

[206] These are technologies «transnational, outsourced, continuously evolving»: see M. Mensi, *Internet, regole, democrazia*, in *Amministrazione in Cammino,* 30 April 2017, and also «transversal, asymmetric and non-territorial»; see. A. Soro, *Liberi e connessi*, Torino, 2016, 76.

[207] M.R. Ferrarese, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo digitale*, Roma-Bari, 2006, 16 ss.

[208] For the doubt over statutory regulation see R. Wacks, *Privacy: A Very Short Introduction*, Oxford, 2012.

[209] The document has been promoted by the Group of European Supervisory Authorities. See M. Betzu, *Regolare Internet. La libertà di informazione e di comunicazione nell'era digitale*, Torino, 2012; F. Cajani-G. Costabile, *Gli accertamenti informatici nelle investigazioni penali: una prospettiva europea*, Forlì, 2012; E. Colombo, *La cooperazione internazionale nella prevenzione e lotta alla criminalità informatica: dalla Convenzione di Budapest alle disposizioni nazionali*, in *Ciberspazio e diritto*, 2009; F. Delfini-G. Finocchiaro, *Diritto dell'informatica*, Torino, 2014; L. Picotti, *La ratifica della Convenzione di Budapest sul Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, Padova, 2008; U. Sieber, *Organized Crime in Europe: the Threat of Cybercrime. Situation Report 2004*, Strasbourg, 2005.

The 2016 EU Regulation has exploited the evolution of data in commodities, using the market as leverage. However, the same change has led to the rise of Data brokers, new economic actors providing data analysis to support direct marketing (detailing)[210] and subjects profiling. While the first practice aims to pin down the data subject's interests so to provide him with more appealing commercials, the latter is even more dangerous and intrusive[211]. In order to limit the data-market the FIPs and Directive 95/46/EC required data-subject agree on his personal information treatment. However, this has soon proven to be an insufficient tool, for two reasons. The first one is the difference "in size" between collectors and users, which results in an "all (your data) or nothing (their services)" approach. The second one is the fact that data analysis resort on unprotected data to obtain, indirectly, personal information. Profilers cross-check apparently innocuous information collected in one or more database. Despite being completely harmless when individually considered, such information if "appropriately" questioned through aggregation enable the data-broker to profile the data-subject. Profiling is not limited to information disclosure, since it aims understand and even foresee the preferences and behaviour of the profiled data subject[212].

This leads us to the next issue, how to prevent data disclosure from the very beginning. The answer is "Pet(s) therapy", better known as Privacy by Design, "PbD") approach. Privacy by design is a concept created in 2009 by Ann Cavoukian, according to whom compliance with regulatory frameworks alone cannot assure privacy substantial protection. It is, therefore, necessary the adoption of Privacy-Enhancing Technologies (Pets)[213]. Softwares and devices specifically designed in order to ensure full transparency and security to data treatment, thus offering privacy an *ex ante* protection[214].

PbD aims to ensure that privacy is taken into consideration by the ICT producers at the earliest stage of the device or software lifecycle. Therefore, it acts as compass setting the direction for a sustainable technological development, rather than a barrier[215].

An example of PbD is the pseudonymisation. It is a data management and de-identification procedure by which personally identifiable information in a data record are replaced by artificial identifiers (pseudonyms). Even if it is suitable for data processing, the data record itself is less identifiable and requires additional information conserved separately to be fully understandable[216]. This procedure is strongly promoted by the

---

[210] This is a very sensitive subject in the US medical context, among many see R.S. Metha, *Why Self-Regulation Does Not Work: Resolving Prescription Corruption Caused by Excessive Gift-Giving by Pharmaceutical Manufacturers*, in *Food and Drug Law Journal*, 63, 2008, 799-802; C.R. Smith, *Somebody's Watching Me: Protecting Patient Privacy in Prescription Health Information*, in *Vt. Law Review*, 36, 2011, 931 and 938-939.

[211] A classic example is Amazon suggesting us books closer to our last views or purchases. See M. Bassini-L. Liguori-O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi*, cit., 333 ss.

[212] S. Gutwirth-R. Leenes-P. de Hert (eds.), *Reforming European Data Protection Law*, New York, 2015.

[213] A. Cavoukian, *7 Foundational Principles of Privacy by Design,* Office of the Information & Privacy Commissioner of Ontario, 2010.

[214] *Ibid.*

[215] D. Klitou, *Privacy-Invading Technologies and Privacy by Design. Safeguarding Privacy, Liberty and Security in the 21st Century*, in *Information Technology and Law Series*, 25, 2014.

[216] Art. 4, no. 5, Regulation (EU) 2016/679.

new Regulation (EU) 2016/679, which offers an integrate view on privacy protection: a digital, legal and organizational one[217]. Another tool is data minimization, according to which only the data strictly related to purpose they are given for can be collected[218]. Minimization is related with both their subsequent use and retention time, which know the same boundary of the purpose for which they had been given for by the data subject.

However, all these measures can easily translate in higher costs for producers and users and this represents the greatest PbD limit. Therefore, to promote their adoption, Regulation (EU) 2016/679 has started considering the Data collector-processor accountable for the eventual risks, thus compelling them to adopt, within the boundaries of proportionality and reasonableness, every mean necessary not to incur in any form of responsibility.

Moreover, the regulation introduces a new form of PbD, a privacy by organization, as it requires certain bodies or corporations to nominate the aforementioned DPO. Afterwards, he will be in charge of promoting privacy protection from within the public body or corporation. Once again, the new regulation has realized the risks posed by a Technological development at the mercy of the Market in a moment when data are a lucrative source of income. Thus, the regulation is trying to exploit the same economic interest that has led to privacy erosion, to the promotion of privacy protection. Forcing the Market to promote privacy-friendly software and hardware for the sake of having access to the European data market.

3.3. The right to be forgotten

Internet has undermined the monopoly on information of traditional media. It has been a two-way process, where the audience is able to collect information by itself and the new media can interact with it directly.

Not only, with the up taking of digital economy, users, while longing for more privacy, feel the urge to share personal content and store data on the web, with little or no clue of the actual risks[219].

One of the most overlooked consequences is the length of their presence on the Internet. Once an information is uploaded, its circulation is subject to the arbitrary parameters of the search engine websites is potentially eternal[220]. Unfortunately for the users, the Web has proved to be unable to govern such a feature, thus requiring the intervention of the Law[221].

---

[217] However, pseudonymised data must not be confused with the anonymized data. See G. Finocchiaro, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Le Nuove Leggi Civili Commentate*, 1, 2017, 1 ss.

[218] R. D'Orazio, *Protezione dei dati by default e by design*, in S. Sica-V. D'Antonio-G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016, 79 ss.

[219] M.C. D'Arienzo, *I nuovi scenari della tutela della privacy nell'era della digitalizzazione alla luce delle recenti pronunce sul diritto all'oblio*, in *Federalismi.it,* 2, 2015, 4-5.

[220] M. Pelligra Contino, *La Corte di Giustizia UE ritorna all'oblio tra diritto alla privacy e diritto ad essere informati: una disamina tra diritto interno e normativa europea*, in *Democrazia e sicurezza,* 23 January 2015.

[221] S. Rodotà, *Il mondo della rete: diritti e vincoli*, Roma-Bari, 2014.

We have already seen that one of privacy features is the capability to exert a control over one's information. Therefore, should users be able to decide, whether or not, to permanently delate their data on the Internet? According to the European institution, yes, thus resulting in the inclusion of the right to be forgotten within the concept of privacy[222]. The right to be forgotten, made popular by Victor Mayer-Schönenberg's book "Delete", is the idea according to which an information should be delated, rather than persist eternally in some database[223]. The first attempt to establish a control over one's own information comes from the Google Spain decision. However, the CJ ruling has raised many concerns, notably those regarding the semi-constitutional role assigned to data-collector[224]. Indeed, search engines, social networks etc. will balance by themselves the conflicting rights to be informed and to be forgotten. Moreover, the data collectors will have to estimate to what extent the right to be forgotten will apply to public figures, which news will address public interests etc. In order to cope with their arbitrariness, the new Regulation 2016/679/EU has established that, whenever a removal request had been denied by the data collector, the data subject must be able to appeal to the national Data Protection Supervisory Authority. The latter has to re-evaluate the conflicting interests and issue a legally binding decision. It dispels the many doubts about the deletion of potentially newsworthy information[225]. Nevertheless, Authorities have shown to be quite sensitive to prone to data-collector demands[226].
Many commentators (especially from the U.S.) have fiercely criticized the right to be forgotten, since it is considered as limiting freedom of expression[227]. However, as other scholars have pointed out, it is no matter of removing completely the data, but rather to modify its indexing[228]. The Regulation does not include any right to be *tout court* delated from the internet would have been too difficult to handle during the balanced reasoning[229].

4. Conclusions

Undoubtedly, advances in technology and civilization have constantly re-shaped the

222 R. Razzante, *I tanti dubbi sul diritto all'oblio*, in *AgendaDigitale.eu*, 7 November 2014; N.L. Richards, *Why Data Privacy is (Mostly) Constitutional*, cit., 1531 ss.

223 N.L. Richards, *ibid.*, 1511 and 1531.

224 CJEU, C-131/12, *Google Spain* (2014), commented by T.E. Frosini, *Diritto all'oblio e internet*, in *Federalismi.it*, 12, 2014, and F. Pizzetti (a cura di), *Il prisma del diritto all'oblio. Il caso del diritto all'oblio*, Torino, 2013, 21 ss.; O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain*, in G. Resta-V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza* Google Spain, Roma, 2016.

225 Centre for Democracy& Technologies, *On the "Right to Be Forgotten": Challenges and Suggested Changes to the Data Protection Regulation*, 2 May 2013.

226 M.C. D'Arienzo, *op. cit.*, 29.

227 N.L. Richards, cit., 1511 and 1531; E. Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, in *Stanford Law Review*, 52, 2000, 1049 and 1115.

228 R. Razzante, *Informazione: istruzioni per l'uso*, Padova, 2014.

229 M.C. D'Arienzo, *op. cit.,* 31.

world around us, bringing new challenges and new vulnerabilities. This has been particularly true for privacy. The digitalization is seriously exposing our personality and private life, setting literally in data, rather than stone, our every act. More than before the details about our lives are no longer ours. Instead, they belong to the companies collecting and processing them and to the government agencies that in the name of our security buy or demand them. Promoting user's awareness of the risks and responsibilities is certainly necessary, but not sufficient. We have already reached the point where data controller can affect the user's decisions and even their self-determination. Technology has proven to be an unyielding force, acting beyond the human boundaries of space and time. However, its strength and resources come from an external source: the market. As long as the market is interested in data-breaching technologies no regulation will be quickly enough to prevent any harm to privacy, thus fulfilling O'Harrow's prophecy that rather than having nothing to hide we will have no place to hide[230]. However, it is premature to call for privacy's death, as it has been predicted even before its birth in XVII century. Over time, the lawyers have always managed to overcome every new challenge to privacy with the most appropriate technical and legal means protections. This is particularly true nowadays, when, instead of building a dam or a breakwater, the actual EU legislation is trying to dig an irrigation channel. This is where resides the brilliance of the Regulation (EU) 679/2016.

Notably, in addition to standardized legislation for the Member-States, it provides many "extra-legal" instruments such as Privacy by Design, Privacy Enhancing Technologies. To better promote their adoption by the data collectors the regulation started considering them directly responsible for the data treated. Moreover, it also requires them to meet the European privacy standards, in order to have access to the European data market.

As a result, the EU is trying to steer the technologic revolution exploiting its reliance on the market, thus controlling it indirectly. The market at the service of privacy. Indeed, this is a concrete and ambitious attempt at turning the tide. If during the first decades of 2000 the Law acted solely after the stimulus of committed privacy violations, now it is finally back to disposing for the future.

[230] R. O'Harrow, *No Place to Hide*, New York, 2006.