Privacy: scepticism, normative approaches and legal protection. A review of the theoretical debate and a discussion of recent developments in the EU

di Elisa Orrù

Abstract: *Privacy: scetticismo, approcci normativi e protezione giuridica. Una rassegna del dibattito teorico e una discussion di alcuni sviluppi recenti nella UE.* Digitalisation has lent the right to privacy increasing philosophical and legal relevance. However, privacy's epistemic status and associated normative values are constantly subject to radical criticisms. This article investigates the validity, in theory and practice, of three radical critiques of privacy. A review of the philosophical and interdisciplinary discourse on privacy during the last half century is followed by analyses of recent legal developments within the EU. Privacy emerges as a highly differentiated and powerful tool to protect individuals and social relations and to limit and redistribute power. However, the right to privacy remains far from realising its practical potential.

Keywords: Theories of privacy, Informational self-determination, data protection, GDPR, right to be forgotten.

1. Introduction

From a legal point of view, and especially from the point of view of EU law and jurisprudence, there seems to be no doubt that privacy and data protection deserve protection as fundamental rights. The right to privacy is not only proclaimed by the Universal Declaration of Human Rights but also protected by regional and national law. In the EU, respect for private and family life and protection of personal data are proclaimed by Articles 7 and 8 respectively of the Charter of Fundamental Rights (CFR). The General Data Protection Regulation (GDPR),[1] moreover, establishes a strong data protection regime, and the Court of Justice of the EU (CJEU) has recently pronounced several decisions that enforce a high level of privacy and data protection.[2]

[1] Regulation (EU) 2016/679 of 27 April 2016.
[2] Judgement of 8 April 2014, case C-293/12 (*Digital Rights Ireland*); Judgement of 13 May 2014, case C-131/12 (*Google Spain*); Judgement of 6 October 2015, case C-362/14 (*Schrems/Facebook*).

Within the philosophical and interdisciplinary theoretical discourse on privacy, however, the value of privacy is not unanimously accepted. Even before privacy began to be widely discussed and advocated for, radical criticisms of the very existence of a value of privacy and a (moral and legal) right to it were being put forth. Beginning with these sceptical views on privacy, advanced by scholars such as Judith Jarvis Thomson and Raymond Geuss, this article reconstructs some of the key aspects of the philosophical and interdisciplinary discourse on privacy during the last half-century. In doing so, it also presents several normative conceptualisations of privacy stressing privacy's value and importance. These include liberal conceptions such as John Stuart Mill's, appraisals of privacy focusing on an individual's freedom of decision such as those advanced by Charles Fried and Anita Allen and finally intersubjective and contextual conceptualisations advocated for by, among others, Priscilla Regan, Stefano Rodotà and Helen Nissenbaum. The paper then turns to some of the most salient aspects of current privacy protection in the context of EU law and jurisprudence. These include GDPR Articles 3 (Territorial scope), 17 (Right to erasure) and 25 (Data protection by design and by default); the EUCJ judgements in the *Digital Rights Ireland*, *Google Spain* and *Schrems/Facebook* cases; and the recent EUCJ Advocate General (AG)'s Opinion on the Passenger Name Record (PNR) Directive. Reconnecting with the radical criticisms of privacy presented at the beginning, the paper goes on to examine whether they are justified, with reference both to theoretical conceptualisations of privacy and to legal measures to enforce the rights to private and family life and to data protection. The paper concludes by maintaining that the various aspects of the right to privacy are, both philosophically and legally, powerful instruments not only to protect individuals from interference but also to preserve core characteristics of social life and to limit and redistribute power. However, important limitations still exist, especially regarding the effective enforcement and realisation of the potential of this rich and complex right.

2. Reductionist and genealogical appraisals

Within the theoretical debate on privacy, reductionist and genealogical approaches question the very possibility of conceptualising privacy as a coherent and unitary concept. From this epistemological impossibility derives, according to these critical appraisals, the uselessness of normative elaborations on the value of privacy and its protection.[3] Privacy, according to these critiques, is too vague and inconsistent a concept, overly influenced by liberalism and its flaws, including an excessive focus on the individual and the (patriarchal) assumption of a clear separation between the private and public spheres. Eminent representatives of this theoretical position are

[3] B. Rössler, *Privatheit*, in S. Gosepath, W. Hinsch, B. Rössler (Eds), *Handbuch der politischen Philosophie und Sozialphilosophie*, Berlin, 2008, 1023–1030, 1027.

US philosopher Judith Jarvis Thomson, British philosopher Raymond Geuss and Swiss cultural and media scientist Felix Stalder.

In the mid-1970s, Thomson published the influential article 'The Right to Privacy', in which she analyses a number of situations in which privacy violations are spoken of and concludes that they would be better described as violations of other, more fundamental rights.[4] These rights include, for example, the right to physical integrity, property rights, and the right over the person, including the right not to be heard or seen in certain situations. Consequently, for Thomson, 'the right to privacy is "derivative" [...]: it is possible to explain in the case of each right in the [privacy] cluster how come we have it without ever once mentioning the right to privacy.'[5] Thus, in her view, the concept of privacy is redundant: it is not only possible, but even desirable for the sake of theoretical simplicity, to dispense with it and focus on the protection of the disparate rights subsumed under its label.

Two and a half decades later, Geuss offered a genealogical deconstruction of the distinction between the private and public spheres, on which, according to him, claims to protect the 'private' rest. In his book *Public Goods, Private Goods*, Geuss elaborates on some historical and contemporary understandings of the concepts 'public' and 'private' to argue that 'there is no single clear distinction between public and private but rather a series of overlapping contrasts'.[6] For Geuss, the importance of the distinction between the public and private realms is usually overestimated; most importantly, the distinction itself is not fixed once and for all. Rather, it is an 'ideological concretion', heavily influenced by liberalism, in which disparate contents from diverse sources have agglomerated, gaining the appearance of self-evident and thoroughly plausible conceptions.[7] Accordingly, there is no distinctive right or good designated by the expression 'right to privacy'. Though the goods protected by privacy safeguards are – Guess concedes – often extremely important, they are not so because they belong per se to the private sphere. Rather, we assign them to this sphere because we already value them as something that should be shielded from intrusion and interference.[8] By adopting a more differentiated and elaborated view of concepts such as 'public' and 'private', Geuss thus seems to suggest, we could also be better able to protect what we consider to be 'goods' in both spheres.

Finally, and with a more marked focus on digitalisation, Swiss cultural and media scientist Felix Stalder took a similar, radically critical position, arguing that privacy is, nowadays, a useless concept.[9] According to Stalder,

[4] J. J. Thomson, *The Right to Privacy*, in *Philosophy & Public Affairs* 4/4, 1975, 295–314.
[5] Ibid., 313.
[6] R. Geuss, *Public Goods, Private Goods*, Princeton, 2001, 6.
[7] Ibid., 10.
[8] Ibid., 107.
[9] F. Stalder, *Privacy Is Not the Antidote to Surveillance*, in *Surveillance & Society* 1, 1 (1 September 2009), 120–24.

the most stringent conceptualisation of privacy to date, namely the concept of informational self-determination, presents privacy as a kind of bubble that surrounds the individual.[10] This view is based on an analogy with physical reality, in which, according to traditional liberal understandings, individuals have the right to decide who may enter their own private spaces (typically their own homes). According to Stalder, this understanding of privacy is deeply rooted in the notion of individualism and in the notion of a human person as an isolated being. Accordingly, privacy is not a suitable means of adequately capturing our reality, which consists of networks, unstable relationships, and dynamic systems of identification. Within this context, we have long since lost control over who has access to our information. Moreover, the 'bubble-like' notion of privacy is incapable of highlighting the implications of surveillance measures in the context of current power relations and limiting them accordingly. Ultimately, the concept transfers 'a 19th century conceptual framework to a 21st century problem.'[11] Thus, even if Stalder's critique focuses on the outdatedness of the concept of privacy rather than on its epistemic status in general, his conclusion is similar to Thomson's and Geuss': to protect values and rights that are generally grouped under the term 'privacy', it would be more effective to focus on strategies other than the legal protection of the rights to privacy or to informational self-determination. These alternative strategies could, for instance, concentrate on ensuring liability in cases of abuse of power connected to surveillance practices.

3. Normative conceptualisations of privacy

In contrast with such radical critiques of privacy, prescriptive approaches to privacy strive to explain its normative content. Within these approaches, three sub-currents can be distinguished: classical liberal theories, contemporary individual-centred conceptions, and intersubjective and contextual theories of privacy.

Classical liberal theories of privacy rely on strict separation between the public and private spheres. Conceptualisations of this kind were first made possible by Thomas Hobbes, who introduced a modern distinction between these two spheres into political thinking. Hobbes' interest, as has been argued, was more to protect the (religious) uniformity of the public sphere from private conflicts than to create a sphere of non-interference from public authority in which diversity could flourish.[12] Nevertheless, in *Leviathan*, he draws a distinction between the public and the private realms that is different from the distinction, prevalent in the Ancient World,

[10] Ibid., 121.
[11] Ibid., 122.
[12] A. Abizadeh, *Publicity, Privacy, and Religious Toleration in Hobbes's Leviathan*, in *Modern Intellectual History* 10, 2 (2013), 261–291.

between the private as the realm of necessity and the public as the realm of liberty.[13] In doing so, he paves the way for later liberal conceptions of privacy that will shift the focus from enabling public uniformity to shielding the private sphere from the interference of public power and society. John Locke's conception of private property as something that 'nobody has any right to but himself'[14] and as including, beyond one's material goods, one's life and liberty as well, is a quintessential example of liberal conceptions of the private sphere within the contractarian tradition.

John Stuart Mill, though outside the tradition of social contract theories, put forth a defence of the private realm as a sphere of intimacy that is often considered to be one of the most insightful liberal conceptions of privacy. For Mill, the most dangerous threats to individuals' liberty no longer derive solely from public power. Even more threatening, in his opinion, are the dangers coming from society:

> Protection [...] against the tyranny of the magistrate is not enough: there needs protection also against the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them; to fetter the development, and, if possible, prevent the formation, of any individuality not in harmony with its ways, and compel all characters to fashion themselves upon the model of its own. There is a limit to the legitimate interference of collective opinion with individual independence; and to find that limit, and maintain it against encroachment, is as indispensable to a good condition of human affairs, as protection against political despotism.[15]

Thus, for Mill, if individuals are to be able to develop their own personality and opinions, they must be able to enjoy a sphere protected from the intrusion and judgement not only of government but also of society.

Contemporary individual-centred conceptions of privacy are clearly influenced by the liberal tradition and ground their definitions of privacy in individuals and their consent or freedom of choice. Within this theoretical framework, privacy is understood either as control over access to information or as inaccessibility, as in the views of US legal scholar Charles Fried and US philosopher Anita Allen respectively. According to Fried, privacy is a necessary precondition for human relationships based on respect, love, friendship and trust. 'Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over

[13] See especially Chapters XVII and XXII of *Leviathan*. For an elaboration on the distinction between the public and the private spheres typical of the ancient world, see H. Arendt, *The Human Condition*, Chicago, 1998.

[14] J. Locke, *Two Treatises of Government and a Letter Concerning Toleration*, I. Shapiro (Ed.), New Haven, 2003, Second Treatise, § 27.

[15] J. S. Mill, On Liberty *in Focus*, J. Gray (Ed.), London, 1991, 26.

information about ourselves'.[16] Privacy thus does not coincide with isolation or secrecy; rather, it consists in a person's ability to 'grant or deny access to others', the ability to exercise control over knowledge about oneself – not just in a quantitative but in a qualitative way, focusing on control over the *kind* of information about oneself that is available to others.[17] Privacy thus conceived is both an aspect of personal liberty and an important means of protecting it.

In her book *Uneasy Access*, Allen approaches the concept of privacy from a feminist perspective.[18] The feminist critique has often stressed the patriarchal aspects entailed by some conceptions of privacy, especially those inspired by the idea of the home as a 'man's castle'. Allen is sympathetic to the feminist critique and agrees with it in stressing that the 'private' space of the home is one in which women do not always experience privacy. Allen does not, however, argue for a wholesale rejection of the idea and value of privacy.[19] Instead, she pleads for a revised conception of privacy whose core element is the ability to control who has access to one's body and thoughts.

To the third category of normative conceptions of privacy belong intersubjective and contextual theories of privacy. These appraisals reject both the strict public/private divide and the exclusive focus on the individual. In contrast, they emphasise the public, political and collective dimensions as well as the interindividual component of privacy.

In the mid-1990s, US political scientist Priscilla Regan argued that an understanding of privacy as an individual value is both disadvantageous and inaccurate.[20] Regan maintains that other values potentially conflicting with privacy, typically including the value of security, are mainly understood as public goods. In the weighing of privacy against these other, 'public' values, privacy is often assigned a weaker position precisely because it is understood 'only' as an individual good. In contrast, Regan argues that privacy is important not only to the individual but also to the community at large. More specifically, privacy is a common, public and collective good. It is a common good because all people value it, even if specific ideas of what exactly privacy is may vary from person to person. It is a public value because it is indispensable to a functioning democratic system. Finally, it is a collective good because, according to Regan, it can only be claimed by one person if, at the same time, all others can also claim a certain minimum of privacy for themselves. Recognising the social value of privacy has important practical implications, allowing it to be seen as a core element of (rather than a potential obstacle to) societal well-being. This perspective

[16] C. Fried, *Privacy. [A Moral Analysis]*, in F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge, 1984, 203–222 (209 here), emphasis original.
[17] Ibid. 210.
[18] A. L. Allen, *Uneasy Access*, Lanham, 1988.
[19] Ibid., 80–81.
[20] P. M. Regan, *Legislating Privacy*, Chapel Hill, 1995.

strengthens the position of privacy whenever a conflict occurs between privacy and some other social value, because privacy is now no longer seen as something that is important only to individuals.

The public importance of privacy stressed by Regan is connected to the influence that real, potential or perceived surveillance practices can have on fundamental rights such as the basic democratic freedoms. This phenomenon, known as the 'chilling effect', consists of a kind of deterrent or inhibition that prevents individuals from exercising their fundamental rights once they know they are under surveillance. The chilling effect has a particular impact on rights that are at the core of democratic life, such as freedom of belief, expression, information, press and assembly.[21] It can lead, for example, to people refraining from taking part in a demonstration because they know that they could be filmed by the authorities while doing so. Similarly, people may refrain from searching for certain content on the Internet in order to avoid being identified as potentially suspicious and thus drawing the attention of the authorities. Recent empirical studies have shown that such an effect can indeed influence the behaviour of Internet users. In the months after the National Security Agency (NSA) surveillance activity became known in consequence of the revelations of its former employee Edward Snowden, for example, searches for certain terms using the Google engine declined.[22] Interestingly, this affects not only terms that can be directly associated with terrorism but also those that are perceived as 'personally sensitive', such as 'abortion'. A study published in 2016 demonstrated similar effects on the use of the online encyclopaedia Wikipedia.[23] In this case, there was a decrease in the frequency with which Wikipedia users read articles perceived to be privacy-sensitive.

Another conception of privacy that decidedly highlights its political dimension is that of Italian legal scholar and first President of the Italian Authority for the Protection of Personal Data Stefano Rodotà. Rodotà has developed a conception of privacy according to which the individual, social and political dimensions are strictly intertwined. His best-known definition of privacy as 'the right to maintain control over one's own information and to determine the modalities of construction of one's own private sphere' partially resonates with the individualistic conceptions of privacy presented above.[24] Yet, Rodotà also stresses that privacy is the term used today to refer to a cluster of powers, spread throughout society, that can offer an effective counterpower to surveillance and the power exercising it only if understood

[21] *The Chilling Effect in Constitutional Law*, in *Columbia Law Review* 69, 5 (1 May 1969): 808–42.

[22] A. Marthews and C. E. Tucker, *Government Surveillance and Internet Search Behavior*, SSRN Scholarly Paper, Social Science Research Network (29 April 2015), https://papers.ssrn.com/abstract=2412564.

[23] J. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, *Berkeley Technology Law Journal* 31, 1 (2016), 117–82.

[24] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, 122, translation by the author.

and practised at social and political levels. Moreover, the existence of public data protection authorities with enforcement duties testifies that privacy not only is conceived as a matter of individual responsibility but also inspires the establishment of institutional obligations to protect it.[25] For individuals, the right to privacy implies the ability to follow the data about themselves, irrespective of the fact that these data are temporarily in the hands of others. By enabling individuals to follow the flows of data about themselves, this right enables them to continue 'governing' these flows.[26] In a certain sense, this conception of the right to the protection of personal data reverses the role that the notion of 'access' plays in liberal definitions of privacy focused on the control over information about oneself, such as the definition defended by Fried. According to Rodotà's conception, access to information is not used 'negatively' by the data subjects to 'keep others out' but rather is claimed actively and positively as their own right to access information about themselves wherever they are.

US computer scientist and philosopher Helen Nissenbaum goes a step further, emphasising not only the social significance of privacy but also its very constitution as a social matter.[27] Following Michael Walzer's theory of 'complex justice', Nissenbaum has developed a theory of privacy as 'complex' privacy. This theory assumes the existence of various social contexts that are neither exclusively 'public' nor exclusively 'private' but represent human interactions that can take place in both the public and the private sphere. Nissenbaum has proposed interpreting privacy as contextual integrity, suggesting that privacy is protected as long as the norms that regulate the flow of information in a given context are respected. Moreover, the dependency of privacy on these norms reveals the social value of privacy: 'These norms, which I call context-relative informational norms, define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power.'[28] It follows that serious violations of privacy threaten not only individual rights but also 'the very fabric of social and political life'.[29] The rootedness of privacy in social norms, moreover, means that it must not be weighed against other values: rather, privacy is itself already the result of a trade-off 'of social rules, or norms, with both local and general values, ends, and purposes'.[30]

4. Privacy in theory and its critics: a provisional assessment

[25] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, in *Laterza* (2014), 31–32.
[26] Ibid., 32.
[27] H. F. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, in *Stanford Law Books*, 2010.
[28] Ibid., 3.
[29] Ibid., 128.
[30] Ibid., 231.

In an article programmatically titled *In Defence of Privacy*,[31] Canadian political scientist Colin J. Bennett addresses several of the most common criticisms of privacy, which partially coincide with the ones presented above and notes that they are based on a misrepresentation of the conventional use of the concept of privacy. Bennett counters the common objection that privacy is a concept too centred on the individual by arguing that understandings characterised by features such as segregation and atomisation are typical of early conceptualisations of privacy. These include, for example, Samuel Warren and Louis Brandeis' first definition of privacy as 'the right to be let alone', presented in a well-known article published in 1890.[32] In Bennett's opinion, this interpretation is not representative, as can be seen from different interpretations of privacy that are currently much more common. The social value of privacy is generally accepted not only theoretically but also in legal and political practice. Similarly, views based on spatial metaphors, such as the bubble-like notion criticised by Stalder, are considered outdated both in the literature and in practice.

In my view, Bennett's claim that the most common criticisms of privacy are based on a misrepresentation is only partially correct. As we saw in Section 3 above, conceptions of privacy as centred on the individual are not confined to the past but are still advanced and defended today. However, it is certainly true that these conceptions do not represent the whole spectrum of privacy conceptualisations. Indeed, understandings of privacy stressing its intersubjective, societal and political character have been prominently put forth for at least the last 30 years, as we have seen. The radically sceptical positions on privacy presented in Section 2 above seem to apply to classical liberal and contemporary individualistic conceptions of privacy, but not to those focusing on its intersubjective, collective and public dimensions. If we consider, for instance, Nissenbaum's conception of privacy, we see that none of the three sceptical positions presented above really challenge the idea of privacy as contextual integrity. Thomson's criticisms lose their grip on this conception because privacy, in Nissenbaum's account, is not understood primarily as a 'right' but as the integrity of a complex set of interrelated norms. Geuss' criticisms focus on conceptualisations of privacy based on a distinction between the private and the public realm, whereas, as we have seen, Nissenbaum's approach does not rest on such a distinction. On the contrary, one of the core themes of her discussions of privacy is the defence of a right to privacy specifically *in public*.[33] Finally, the 'bubble-like' conception of privacy criticised by Stalder clearly does not

[31] C. J. Bennett, *In Defence of Privacy: The Concept and the Regime*, in *Surveillance & Society* 8, 4 (24 March 2011), 485–96.
[32] S. D. Warren and L. D. Brandeis, *The Right to Privacy [the Implicit Made Explicit]*, in F. D. Schoeman (Ed.), *Philosophical Dimensions of Privacy*, cit., 75–103.
[33] H. Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, in *Law and Philosophy* 17, 5–6 (1998), 559–596.

apply to theories, such as Nissenbaum's, that stress the intersubjective and societal dimensions of the concept.

In his defence of privacy, Bennett not only rejects criticisms of the concept of privacy but also focuses on common objections to privacy as a legal entitlement. As a legal right, privacy has been criticised as inappropriate for protecting the most vulnerable social groups because it is too abstract and too difficult to enforce. To these objections, Bennett responds that lawsuits are not the only way to enforce privacy. Privacy agencies can also effectively investigate individual complaints and pursue broader questions of principle. Finally, privacy critics contend that the core problem with data collection and aggregation is not so much about privacy as it is about discrimination. Surveillance, they argue, serves as a 'social sorting' tool, distinguishing people not so much on the basis of individual characteristics as on the basis of their presumed membership in certain groups.[34] To this objection, Bennett responds that this form of surveillance risk has long been considered part of privacy protection measures and mechanisms. Special protection is given to sensitive data, such as information that can reveal ethnicity, gender, age, health status, political opinion, and religious or philosophical beliefs. On the basis of these considerations, Bennett concludes his defence of privacy as follows:

[Privacy] as a concept, as a regime, as a set of policy instruments, and as a way to frame advocacy and activism, […] displays a remarkable resilience as a way to regulate the processing of personal information by public and private organizations, and as a way for 'privacy advocates […] to resist the excessive monitoring of human behaviour.[35]

Whether we can follow Bennett in his optimistic view of the legal force of privacy in protecting core human values is a matter I would like to address after presenting recent developments in privacy-related EU law and jurisprudence.

5. The legal dimension: private life and data protection in the CFR of the EU

The CFR includes two articles protecting different aspects of privacy. Article 7, *Respect for private and family life*, establishes that '[e]veryone has the right to respect for his or her private and family life, home and communications'. Article 8, *Protection of personal data*, focuses on informational privacy, that is, privacy regarding information about one's person. The article reads:

[34] See O. H. Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, Boudler, 1993, and D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, London, 2003.

[35] Bennett, *In Defense of Privacy*, op. cit., 495.

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.

While Article 7, as noted above, protects the traditional spheres of family life, the home and communication from undue interference, Article 8 establishes the right of data subjects to actively control the flow of data regarding their person.[36]

6. Privacy by Design and the GDPR

The concrete modalities for protecting the fundamental rights to privacy and data protection in the EU are specified in the GDPR, which was adopted in April 2016. The GDPR devotes attention not only to typical legal aspects but also to technical measures of data protection. Its Article 25 makes 'data protection by design and by default' mandatory for any person or organisation responsible for processing personal data. Privacy by Design (PbD) is an approach that aims to build privacy protection mechanisms into the development of new technologies. The core idea is that the earlier these mechanisms are used in the development process, the more effective they are. The foundations of PbD emerged in the 1990s from a collaboration between the Dutch Data Protection Authority and the Freedom of Information and Privacy Commissioner of the Canadian province of Ontario, Ann Cavoukian.[37] Cavoukian has since developed the concept and identified seven key principles of PbD.[38] These stipulate, among other things, that measures to protect privacy should be used as basic settings as early as possible during the development of new technologies. Furthermore, one of the basic principles of the PbD model is that privacy protection does not reduce the functionality of the technological system and that, accordingly, no conflict exists between privacy protection and other values such as security. Moreover, the basic principles establish that privacy protection measures should accompany the whole data processing cycle, from data collection to data deletion, that transparency and accountability must be ensured and that users' interests should be prioritised. Cavoukian herself and

[36] S. Pietropaoli, *Privacy e oblio. La protezione giuridica dei dati personali*, in F. Faini and S. Pietropaoli, *Scienza giuridica e tecnologie informatiche*, Torino, 2017, 41–66 (48 here).
[37] P. Hustinx, *Privacy by Design: Delivering the Promises*, in *Identity in the Information Society* 3, 2 (2010), 253–55.
[38] A. Cavoukian, *Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era*, in O. M. G. Yee (Ed.), *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*, Hershey, 2012, 170–207.

her collaborators have designed technological systems that put these principles into practice. However, the broader engineering community has also developed a variety of applications that, while inspired by PbD principles, sometimes differ significantly from – and offer stronger privacy safeguards than – the applications proposed by Cavoukian.[39] Nowadays, therefore, PbD is understood to mean, on the one hand, the 'official' basic approach developed by Cavoukian herself, and, on the other hand, a wide range of concrete applications that differ greatly from one another.

Article 25 of the GDPR, as mentioned, establishes PbD and privacy by default as core principles of data processing:

4. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

5. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

Similar duties are also included in Directive 2016/680, which regulates data protection in the context of police and judicial cooperation (Article 20).

7. Rulings of the CJEU on private companies' data processing and Articles 3 and 17 of the GDPR

In 2014, as the GDPR draft was being negotiated, the CJEU issued two prominent rulings in favour of extensive privacy protection.[40] These are the

[39] See for instance C. Diaz et al., *Privacy Preserving Electronic Petitions*, in *Identity in the Information Society*, 1, 1 (1 December 2008), 203–19; J. Balasch et al., *PrETP: Privacy-Preserving Electronic Toll Pricing*, in 19th USENIX Security Symposium (USENIX Association, 2010), 63–78; C. Bier et al., *Enhancing Privacy by Design from a Developer's Perspective*, in B. Preneel and D. Ikonomou (Eds), *Privacy Technologies and Policy*, *Lecture Notes in Computer Science 8319*, Berlin, 2014, 73–85.

[40] On these judgements, see also S. Pietropaoli, *Privacy e oblio*, cit.; N. Miniscalco, *La personalità in rete: protezione dei dati personali, identità digitale e diritto all'oblio*, in Th.

decisions in the two cases of *Google Spain* and *Schrems/Facebook*, whose core elements align with GDPR Articles 17 and 3 respectively.

In the *Google Spain* case, the Court had to judge whether the operator of a search engine must consider a request by individuals to remove links to web pages presented as results of a search performed by entering their names, and under what conditions the operator must accept such a request. In its decision of 13 May 2014, the CJEU ruled that

> the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful (§ 4).

According to the Court's decision, the duty to remove the related links applies whenever the information displayed is 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue' (§5). The responsibility of the search engine operator stands, according to the Court, independent of the fact that the data have already been published on the internet (§1). Moreover, the processing performed by the search engine operator

> enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him. That is all the more the case because the internet and search engines render the information contained in such a list of results ubiquitous (§2).

A similar approach emerges from Article 17 of the GDPR, *Right to erasure ('right to be forgotten')*. This Article establishes that

> 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

Casadei, S. Pietropaoli (Eds), *Diritto e tecnologie informatiche*, Assago, 2021, 31–44; and J.-P. Schneider, *Recent Developments in European Data-Protection Law in the Shadow of the NSA Affair*, in R. Miller (Ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge, 2017, 539–563.

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

The ruling of the EUCJ in the *Google Spain* case is, moreover, connected to Article 22 of the GDPR, *Automated individual decision-making, including profiling*. This article does not prohibit profiling absolutely, but only in specific cases and only if the profiling leads to a decision based *exclusively* on automated decision-making. It additionally prohibits (though again with exceptions) profiling activities based on sensitive data:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

In a similar vein, Article 11 of Directive 2016/680, which regulates data protection in the context of police and judicial cooperation, establishes

comparable limitations and duties, which also apply when the data are processed by public authorities in criminal law matters. This Directive, however, places additional emphasis on the prohibition of discrimination, as it provides that

3. Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

The second prominent case ruled on by the CJEU concerning the processing of personal data by private companies is known as *Schrems/Facebook*. The case concerned a complaint made by an Austrian citizen, Maximilian Schrems, before the Irish supervisory authority. Schrems claimed that personal data transferred by the Irish Facebook subsidiary to Facebook servers located in the United States were not sufficiently protected. Schrems grounded his claim in the revelations made by Snowden, which revealed that a pervasive surveillance program had been put in place by the US NSA. The Irish supervisory authority rejected his claim by arguing that the 'safe harbour' scheme, regulating the transfer of data between the EU and the US, provided adequate safeguards. The 'safe harbour' scheme was established by the EU Commission's Decision 2000/520, which established personal data transferred from the EU to the US were to be considered to enjoy a level of protection in line with EU standards.

The CJEU, relying on a reference made by the High Court of Ireland, found in its decision of 6 October 2015 that the 'safe harbour' scheme was not capable of guaranteeing effective protection of the right to privacy and declared Decision 2000/520 to be invalid.

One central argument on which the Court grounded its decision refers to an assessment carried out by the EU Commission in which it

found that the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased (§90).

Article 3 of the GDPR, *Territorial Scope*, is very much in line with this ruling in establishing that

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

8. The EUCJ and surveillance by public authorities: the ruling on the Data Retention Directive and the AG Opinion on the PNR Directive

A final CJEU decision of particular interest for the purposes of this article is the judgement of 8 April 2014 that invalidated Directive 2006/24/EC on data retention. The Data Retention Directive obligated Member States to issue regulations to ensure that communication service providers retained for a minimum of 6 months and a maximum of 2 years the traffic data they managed (Article 6). In particular, providers had, according to the directive, to retain the data necessary to identify the source, destination, time, date, duration and type of communication along with the type of equipment used and its location. Data concerning the content of the communication were explicitly excluded from the categories of data to be retained (Article 5). The purpose of the directive was to ensure the availability of the retained data 'for the investigation, detection and prosecution of serious crime' (Article 1).

In the case known as *Digital Rights Ireland*, the CJEU was asked to examine whether the Directive was compatible with the Charter of Fundamental Rights of the EU – not only with Articles 7 and 8 but also with Article 11, which guarantees the right to freedom of expression and freedom of information. The Court recognised that

> it is not inconceivable that the retention of the data in question might have an effect on the use, by subscribers or registered users, of the means of communication covered by that directive and, consequently, on their exercise of the freedom of expression guaranteed by Article 11 of the Charter (§ 28).

However, the CJEU decided not to answer directly the question whether the Directive was in conflict with freedom of expression and information and to concentrate instead on the Directive's compatibility with respect for private and family life and the protection of personal data. Having

asserted that the Directive was to be considered invalid with respect to Articles 7 and 8 of the Charter, the Court saw no need to discuss further the compatibility of the Directive with Article 11 (§ 69–70). Thus, although the CJEU did not rule out the possibility that the data retention provided for in the Directive could lead to restrictions on the freedoms mentioned, the judges limited the compatibility test only to the privacy-related Articles 7 and 8.

The Court, in its judgement, nevertheless also discussed aspects of the case closely related to freedom of expression and information. Indeed, it expressed concerns regarding the feeling of being under surveillance and the 'chilling effect' this feeling can have on subjects.

In particular, the Court stated that

> the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (§37).

The CJEU furtherly referred to the Opinion of December 2013 by the AG, in which he recalled a previous decision by the German Constitutional Court on the Data Retention Directive and affirmed that

> the vague feeling of surveillance which implementation of Directive 2006/24 may cause is capable of having a decisive influence on the exercise by European citizens of their freedom of expression and information.

The German Constitutional Court, in its previous ruling of 2 March 2010,[41] stressed the fact that such surveillance activity 'might generate a diffuse and threatening feeling of being watched, which in turn may compromise the unprejudiced enjoyment of fundamental rights in many domains' (§212). Moreover, the judges argued that the vagueness of surveillance measures aggravates this chilling effect

> because it can generate a feeling of constantly being under surveillance; it provides profound insights into private life in an unpredictable way, without making the recourse to the data directly noticeable or evident. Individuals neither know which state authority knows something about them nor what they know, but they know that the authorities can have a lot of knowledge about them, including highly personal information (§241).

Whether the CJEU will stick to this line of argument in another case currently under consideration, namely the one concerning Directive (EU)

[41] Judgement of 2 March 2010, Nos. 1 BvR 256/08, 1 BvR 263/08 and 1 BvR 586/08; translations of quoted sentence passages by the author.

2016/681, also known as the PNR Directive, is still an open question. Interestingly, AG Pitruzzella, in his Opinion provided on 27 January 2022, maintains that recent decisions on data retention measures by the EUCJ do not apply to the PNR case. AG opinions are not binding for the Court. Indeed, in past decisions, while the Court has sometimes decided to follow most of the argumentation in the AG's opinion (as in the ruling on the Data Retention Directive), at other times its decisions have rested on a very different basis (as in the *Google Spain* case). It is nevertheless interesting to recall some of the main arguments advanced by the AG.

The PNR Directive requires that the data of all those who book an extra- (and optionally intra-) European air flight be collected, saved and sent to central national systems of Member States typically managed by police authorities. The data collected on the basis of the PNR Directive concern the method of payment for the air ticket, the travel itinerary, the travel agency making the booking, the seat occupied on the plane, any accompanying persons or travel companions, the luggage and an unspecified category of 'general remarks'. The data are retained by the national unities for a period of five years.

The AG concludes that 'the transfer and the *generalised and undifferentiated* automated processing of PNR data are compatible with the fundamental rights to respect for private life and to the protection of personal data'.[42] This, however, does not apply, in the AG's assessment, to the *retention* of the data:

> By contrast, a generalised and undifferentiated retention of PNR data in a non-anonymised form can be justified only where there is a serious, actual and present or foreseeable threat to the security of the Member States, and only on condition that the duration of such retention is limited to what is strictly necessary.[43]

Additionally, the category of data labelled 'general remarks' is not clear and precise enough to meet the requirements of Articles 7 and 8 of the CFR, and the relative provisions must be declared invalid (§ 254). All other categories of data are, according to the AG's Opinion, relevant and adequate, and the requirements of necessity and proportionality of processing are met (§233), given that, among others, the processing of sensitive data is explicitly prohibited by the Directive. However, according to the AG, limits should apply to the modalities through which data are processed. The use of machine learning techniques to adapt the criteria according to which the

[42] Court of Justice of the European Union, Press Release No. 19/22, Luxembourg, 27 January 2022, Advocate General's Opinion in Case C-817/19, *Ligue des droits humains*, 1 (emphasis added).

[43] Ibid. See also *Conclusions de l'Avocat Général M. Giovanni Pitruzzella présentées le 27 janvier 2022* (1) Affaire C-817/19, *Ligue des droits humains contre Conseil des ministres* (to date available only in French), § 241.

individual risk of passengers is assessed should be prohibited if that use makes it impossible to understand the reasons that have led to a given assessment (§228).

9. Privacy in practice: final considerations

A differentiated consideration of existing conceptions of privacy shows, as we saw in Section 4 above, that the conceptual criticisms of privacy examined here do not apply. Existing conceptions of privacy are far more complex, rich and apt for describing violations of basic moral and legal rights than their radical critics hold. Having examined key legal instruments for the protection of privacy in the EU, I now turn to the still unanswered question of Section 4 above, namely whether the criticisms presented apply to the legal dimension of privacy.

According to Thomson, as we have seen, the right to privacy is derivative, in the sense that what it aims to protect can be always described in terms of the protection of other rights. Granted, the set of EU legal instruments presented in sections 5–8 above allows for the conclusion that the rights to privacy and data protection have strong connections to other rights. These include, as we have seen, basic freedoms of expression and information, and, in the legal systems that recognise it, the right to (digital) personal identity.[44] However, the rights to privacy and data protection have shown the ability to cluster claims of protection against violation in a way that would not be possible if these two rights were not formally recognised. For instance, in the prominent decisions on the *Google Spain* and *Schrems/Facebook* cases, there is clearly no other right in the CFR of the EU that could have served the purpose.

The criticism advanced by Geuss, as seen above, focuses on the distinction between the public and the private sphere, which Geuss views as misleading. However, the legal rights to privacy and data protection rest on this distinction only in part. The right to data protection, in particular, seems to explicitly disregard the question whether the personal data to be protected are located in a 'private' or 'public' sphere, no matter how these are defined. In the *Google Spain* case, indeed, the CJEU explicitly stated that if the relevant conditions apply, the duty to remove the links holds even when the data are legally published in other venues on the web. If the right to data protection were based on a strict distinction between the public and private spheres, this interpretation would have not been possible. In that case, the right to data protection would protect personal information only insofar as the information to be protected was kept in the 'private' sphere; it would no longer apply to information already in the public sphere. The same considerations hold for the right to erasure according to Article 17 of the

[44] Concerning the Italian legal system, see N. Miniscalco, *La personalità in rete*, cit., 40.

GDPR, which applies irrespective of whether the data were previously published in a 'public' or publicly accessible venue.

Finally, the core of Bennett's critique of the right to informational self-determination, understood as the most advanced conception of privacy, attaches to the alleged understanding of privacy as a 'bubble' surrounding an individual to guarantee a sphere of non-interference. However, current enforcement of the right to private life and data protection, at least in the EU, focuses precisely on information *flows*. At all levels of protection of these rights (CFR, GDPR and judgements of the CJEU), the fundamental premise is not that data should be kept in a sphere inaccessible to others in order to be protected, but that personal information flows and that legal protection shall apply *while it flows*. The *Schrems/Facebook* judgement and Article 3 of the GDPR are probably the most illustrative examples of this among the cases discussed in Sections 5–8 above. Indeed, the judgement of the Court and the related GDPR legal provisions aim to guarantee the protection of data that have been made available by the data subjects themselves (and thus are flowing between them and Facebook and other Facebook users) and extend this protection to data that flow over the Atlantic Ocean or elsewhere outside the territory of the EU.

One additional aspect of Stalder's criticism mentioned above concerns the ability of privacy to protect against power abuses. As we have seen, however, privacy and data protection have proven to be useful tools for limiting and redistributing power. The requirements of necessity and proportionality for the processing of personal data, which should be considered in assessing the impact of data processing activities according to Article 38 of the GDPR and to which the EUCJ refers in its judgement (see for instance the judgement's excerpts in the *Schrems/Facebook* case above), clearly aim to restrict the power of the entities processing the data. Furthermore, some requirements of the 'privacy by design and by default' approach, such as data minimisation and the need for the subject's active action as default settings for data processing, aim to counterbalance the power of data processors over data subjects.

Can we then share Bennett's optimistic conclusions about the legal force of the concepts of privacy and data protection?

In my view, notwithstanding the abovementioned merits of the rights to privacy and data protection, several limitations are still in place. These concern the ability of privacy to limit and redistribute power not only in the social but also in the political sphere and the protection that these rights can provide against 'social sorting' practices.

Regarding the first point, it must be noted that, regrettably, no requirements equivalent to the assessment of necessity and proportionality established by Article 35 of the GDPR are set by Directive 2016/680 on data protection in the context of police and judicial cooperation. The Directive only recalls in its preliminary considerations that all data

processing by police and judicial authorities must be 'laid down by law and constitute a necessary and proportionate measure in a democratic society' (recital 26). Additionally, the *Digital Rights Ireland* case, as we have seen, entailed the opportunity for the CJEU to elaborate on the political relevance of privacy by focusing on the compatibility of the Data Retention Directive with Article 11 of the CFR EU, protecting freedom of expression and information. The Court, indeed, stated that surveillance practices are able to induce the so-called chilling effect with detrimental implications for fundamental freedoms, but it refrained from deciding on the Directive's compatibility with Article 11.

Similarly, the potential effectiveness of the right to privacy in protecting the most vulnerable groups against discrimination is still limited. This does not mean that privacy and data protection are rights of the privileged. As Stefano Rodotà convincingly argued, although the origins of the right to privacy are rooted in the milieu of the US high *bourgeoisie*, 'later on, privacy revealed its social side [as the …] right of political, cultural and social minorities not to be discriminated against for their opinions, habits or customs'.[45] The case of the major Italian automaker Fiat holding 'personal files' on their employees and aspiring employees that included information, provided among others by the 'Carabinieri' and parish priests, about their political opinions and affiliations, trade union membership, religious habits and even marital fidelity, which came to light in 1971, is an example of the scope of the value of privacy specifically for socially or economically disadvantaged groups.[46] Nevertheless, the mechanisms for enforcing this right are still difficult to access – and even more so for the most vulnerable groups. Only the privileged few have the cultural, financial and time resources to resort to legal suits, and even if successful, these legal resorts exhibit their effects only years after a legal action has been started. Individual complaints about the use of personal data are, additionally, decided in most cases by the data processors themselves, as is the case with requests addressed to Google to execute individuals' right to erasure.[47] Furthermore, when existing regulations empower national and local data protection authorities to enforce particular guarantees, these entities are often not equipped with the necessary material and personal resources to deal effectively with data subjects' complaints if these subjects were to make widespread use of their rights to complain. For instance, when the PNR Directive was put in place in Germany, 628 new public servants were estimated to be needed for dealing with the new data processing tasks. Yet, only 4 of these new positions were allocated to the Federal Data Protection

[45] S. Rodotà, *Intervista su privacy e libertà*, Roma-Bari, 2005, 9–10, translation by the author.
[46] Ibid., 26–27.
[47] 'Google judex in causa sua', as Pietropaoli efficaciously puts it in S. Pietropaoli, *Privacy e oblio*, cit., 57–65.

Agency.[48] Considering that the PNR Directive potentially affects all passengers of intra- and extra-EU flights, this number seems inadequate to deal with potential complaints in case of a widespread exercise of the right to complain before the Data Protection Authority.

Finally, as we have seen, both the GDPR and Directive 2016/680 set out a prohibition on profiling that is qualified and relative. In consideration of the possibilities opened up by big data and artificial intelligence techniques, a prohibition on using sensitive data for profiling is not a sufficient safeguard against potential discrimination resulting from data processing since sensitive information can easily be derived by non-sensitive 'proxies', such as zip code for ethnicity.[49]

As we have seen, moreover, even if the CJEU has been very sensitive to the complex dimensions and implications of privacy and data protection, this line of interpretation cannot be taken for granted. The recent AG Opinion in the PNR case, indeed, shows that the complexity and richness of these two concepts are not always made fully operative in legal assessments.

To conclude, the rights to privacy and data protection have proven to be utmost multidimensional and potentially apt to protect not only the 'private' and intimate sphere of each individual but also fundamental social relationships and the proper functioning of a democratic system. The concept of privacy is a flexible conception that has evolved over time to adapt and respond to sociotechnical transformations. Critiques dismissing the entire concept of privacy thus often rely on *pars pro toto* misrepresentations and neglect the richness and complexity of the concept. Privacy protection, however, cannot always express its full potential due to limitations inherent in the mechanisms and instruments available to enforce it.

[48] L. Ulbricht, *When Big Data Meet Securitization: Algorithmic Regulation with Passenger Name Records*, in *European Journal for Security Research*, 3 (2018), 139–161 (156 here).
[49] E. Orrù, *Minimum Harm by Design. Reworking Privacy by Design to Mitigate the Risks of Surveillance*, in Leenes, Ronald et al. (Ed.), *Computers, Privacy and Data Protection: Invisibilities & Infrastructures*, Berlin 2017, 107–137 (129 here).