unesco

Guidelines for Judicial Actors on Privacy and Data Protection

These guidelines aim to provide a general framework for judicial actors to assess matters of privacy and data protection in the face of other rights, such as freedom of expression and the right to privacy. The document includes relevant case law from various national, international and regional bodies that may inform judicial actors' understanding of the matters at hand. It draws a coherent line from privacy rights to data protection rights and the challenges of upholding these rights in the face of new technologies.

Introduction: foundations and limitations of privacy rights

These guidelines aim to provide a general framework for judicial actors to assess matters of privacy and data protection in the face of other rights, such as freedom of expression and the right to privacy. New technologies are increasingly key to define the ways citizens relate to information, and often put forward situations where the balance between rights such as privacy and freedom of expression need to be carefully examined by judicial actors.

Technology, indeed, contributes to add more complexity to this context. Informational rights, such as privacy, access to information, freedom of expression and others, should today be considered by their intrinsic value but also as instrumental rights, as they enable several other rights and liberties that increasingly depend on information and communication technologies to be fulfilled. In such a scenario, privacy and data protection, other than opposed, should be considered as complementary to freedom of speech.

In these guidelines, reference will be made to international standards and case law on privacy and data protection, which will serve as a starting point to structure the *ratio decidendi* (the rationale for the decision) and *ratio legis* (the reason for the law) behind the treatment of such rights in different jurisdictions and regional, international and supranational bodies. We will seek to explore the human rights foundations of privacy, its distinction and close relation to data protection and informational self-determination[1] and the areas where these rights clash or resonate with freedom of expression and other human rights. This will allow the reader to understand the subject as a whole, as well as to draw conclusions on how to apply these rights in practice.

[1] See more: The notion of informational self-determination plays a fundamental role on the development of data protection legislation. It derives from Alan Westin's idea as being "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (...) [It is] the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others", which was further elaborated and applied as the **Informationelle Selbstbestimmung** concept by the German Federal Constitutional Court in 1983, which defined it as "the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others".

These guidelines will also identify pressing issues in the juxtaposition of privacy, data protection, freedom of expression and other human rights. Thus, they will draw on reports and studies to identify areas where the tension between these rights requires careful legal analysis, such as the use of surveillance technologies for investigative and national security purposes, assurances of press freedom in the face of the privacy rights of individuals, the protection of journalists and their sources, access to public data, and cross-border data flows.

1.1 Right to privacy and private life

The right to private life is recognized by various international human rights instruments, such as the 1948 Universal Declaration of Human Rights (art. 12), the 1966 International Covenant on Civil and Political Rights (art. 17), the 1990 International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (art. 14), the 1989 Convention on the Rights of the Child (art. 16), the American Convention of Human Rights (Pacto de San José, art. 11.2), the European Convention on Human Rights (art. 8), the African Charter on Human and Peoples' Rights,[2] the Arab Charter on Human Rights (art. 16, 8) and the ASEAN Human Rights Declaration (art. 21).[3]

The concepts of privacy and private life are frequently used interchangeably. Article 12 of the Universal Declaration of Human Rights (UDHR) paints a particularly precise image of the conceptual plasticity of "privacy" and "private life". Between 1946 and 1948, the UDHR drafting effort took place in various fora and, regarding privacy and private life, the different versions of Article 12 reveal a multiplicity of interpretations and uses. "Privacy" and "Private life" were used at times as umbrella terms covering many aspects of the private sphere and in other instances as specific protections for family life and the home.[4] Interestingly, many of the aspects touched upon leading to the final text of Article 12 of the UDHR have since then become the object of decisions by regional courts in the matter of privacy and private life - namely, the protection of home, correspondence, honour and reputation and, more broadly, of the "person".

[2] The African Charter on Human and Peoples' Rights does not contain a provision on the right to privacy. However, it has been argued that the right can be read into the African Charter through the right to respect for life and integrity of the person, the right to dignity, and the right to liberty and security of the person. Singh and Power, 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa', African Human Rights Yearbook 3 (2019) 202.

[3] The three last instruments do not carry substantial enforceable weight.

[4] Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a human right. Human Rights Law Review, 14(3), 441–458. https://doi.org/10.1093/hrlr/ngu014

The right to privacy is furthermore explicitly cited by documents such as the Charter of Fundamental Rights of the European Union (CFR), the Asia-Pacific Economic Cooperation (APEC) Privacy Framework and the Declaration of Principles on Freedom of Expression and Access to Information in Africa, adopted by the African Commission on Human and Peoples' Rights (ACHPR). The latter cites, in its Preamble, "that freedom of expression and privacy are mutually reinforcing rights that are essential for human dignity and the overall promotion and protection of human and peoples' rights",[5] which gets to the crux of this complex web of human rights: human dignity and, consequently, the development of personality and personality rights. Privacy is as well at the root of the Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS)[6] and the African Union's (AU) provisions on data protection contained within its Convention on Cyber Security and Data Protection,[7] alongside various efforts to harmonize privacy and data protection rules in Africa's Regional Economic Communities[8].

2. Balancing rights: the proportionality principle

Seldom is the right to privacy considered and applied without the consideration of other bordering rights, that must be all proportionally considered. The proportionality principle, the main tool for this task, is deeply rooted in the idea of human dignity. Born out of the post-WWII German constitutionalism,[9] it influenced the jurisprudence of the European Court of Justice (ECJ) —which recognizes it as a general principle of law[10]— the European Court of Human Rights (ECtHR), the African Court on Human and Peoples' Rights (AfCHPR) and the Inter-American Court of Human Rights (IACtHR).

[5] https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf, p. 9.

[6] ECOWAS, 'Supplementary Act on Personal Data Protection within ECOWAS' (16 February 2010) http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED-Data-Protection-Act.pdf accessed 1 February 2022.

[7] African Union, 'Convention on Cyber Security and Personal Data Protection' (27 June 2014) https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf accessed 1 February 2022.

Proportionality comes into play when two human rights are at odds. Then, a balancing test needs to be made, which is based on the principle of proportionality. This usually concerns interferences of the State into the rights of individuals, thus frequently translating into an opposition between collective and individual interests. The proportionality test is explicitly applied in the context of the European legal systems (ECJ and ECtHR), the African regional legal framework (AfCHPR), the East African Court of Justice (EACJ), and the American regional human right system (IACHR), and has been gaining space in various decisions of the Human Rights Committee (HRC).

In broad strokes, the proportionality test revolves around three steps: suitability (whether the interference is actually suited to achieve the alleged aim), necessity (also "less restrictive alternative" or "minimal impairment"; whether the measure taken is the least restrictive alternative) and proportionality in the strict sense (whether the benefits achieved are outweighed by the limitations caused). It is also usually preceded by two additional tests of legality (whether the interference is based on national law) and legitimate aim (whether the interference pursues one of the aims dictated by the limitation clauses present, respectively, in the Covenant on Civil and Political Rights (ICCPR), ECHR, ACHPR or AfCHPR).[11] In specific regional systems, these tests take on distinct characteristics.

The European Court of Human Rights follows the 3-part test to establish a violation of the privacy rights afforded by Article 8 of the Convention. These are based on the concepts of **lawfulness**, **legitimacy** and **necessity in a democratic society**.

Lawfulness refers to the existence of a previous and accessible law, enacted through a valid process that authorizes the actions of the particular person or authority. In other words, the interference needs to be based on domestic law that is accessible (***Shimovolos v. Russia***), foreseeable (***Rotaru v. Romania***) and accompanied by effective "safeguards [against abuse] established by law"[12] (***Rotaru v. Romania***). According to the ECtHR in ***L.H. v. Latvia***, there should be, in summary, a "domestic law, which

[8] Graham Greenleaf and Marie Georges, 'African Regional Privacy Instruments: Their Effects on Harmonization' (2014) 132 Privacy Laws and Business International Reporter http://ssrn.com/abstract=2566724 accessed 1 February 2022.

[9] Dinah, S. (Ed.). (2013). *The Oxford Handbook of International Human Rights Law* (1st ed.). Oxford University Press. https://doi.org/10.1093/law/9780199640133.001.0001

[10] Idem, p. 371.

[11] Idem, p. 372.

[12] Rotaru v. Romania, paragraph 59. https://www.bailii.org/eu/cases/ECHR/2000/192.html

should be compatible with the rule of law, which, in turn, means that the domestic law must be formulated with sufficient precision and must afford adequate legal protection against arbitrariness".[13]

The second part in the test, legitimacy, refers to the ends of the action—if they pursue a legitimate function regarding the Convention. This is determined by Article 8 (2) of the Convention, namely: national security; public safety; the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals; or for the protection of the rights and freedoms of others.

Finally, necessity is characterised in the absence of a less restrictive alternative and, in this case, also resonates with elements of strict proportionality as it compares the potential impact of the action on rights to the potential benefit derived from it. The proportionality test in the jurisprudence of the ECtHR puts great weight in proportionality in the strict sense, with suitability and necessity coalescing into either the third part of the test or the two preliminary analytical parts.

For example, in ***Friedl v. Austria***, on the matter of necessity in a democratic society, the Commission stated in its report regarding the case that the keeping of criminal records can be regarded as necessary for the prevention of crime, and that, *in casu*, the record was maintained in a way ("the police did not seek to establish the identities of the demonstrators [...], the personal information recorded and the photographs were not entered into a data-processing system") such as to not disproportionately interfere with the subject's right to privacy.[14]

It is interesting to note in ***Friedl v. Austria*** that not only the gravity of the potential harm that gives rise to the interference on one's private life, but also the mitigating factors (data was "not entered into a data processing system") and proportion of the interference are taken into account. This derives in part from the notion that the strict proportionality analysis is context-specific; it aims at balancing rights "in a particular factual setting".[15] This is a difficult balancing decision that must be taken carefully by the judicial decision-maker: how far can an interference go to pursue a legitimate, lawful goal before it becomes exaggerated?

[13] L.H. v. Latvia, paragraph 47. https://uniteforreprorights.org/wp-content/uploads/2017/12/CASE-OF-L.H.--LATVIA1.pdf
[14] Friedl v. Austria, paragraph 8. https://www.bailii.org/eu/cases/ECHR/1995/1.html
[15] Dinah, S. (Ed.). (2013). *The Oxford Handbook of International Human Rights Law* (1st ed.). Oxford University Press. https://doi.org/10.1093/law/9780199640133.001.0001, p. 373.

Many cases illustrate this analysis, among which we might highlight the following. For example:

- In ***S. and Marper v. the United Kingdom***, a policy of indiscriminate retention of biometric data of investigated persons, even after their acquittal, was found not to meet these criteria. It was deemed disproportionate and risky due to there being no time limit and its indiscriminate nature, and the State could not demonstrate that there were no alternatives, less invasive means to achieve the same goal.[16]
- In ***L.L. v. France***, the European Court dealt with the challenge of judging a matter that is, by its own nature, an interference with private and family life: a divorce. In the case, one of the spouses provided documents to the Court concerning the other spouse's health. The admission of this information before the national court was deemed as an interference in the spouse's right to privacy. The Court found that "the impugned interference with the applicant's right to respect for his private life, in view of the fundamental importance of the protection of personal data, was not proportionate to the aim pursued and was therefore not "necessary in a democratic society for the protection of the rights and freedoms of others"[17]. In this regard, the European Court found that "it was only on an alternative and secondary basis that the domestic courts used the disputed medical document in justifying their decisions, and it thus appears that they could have declared it inadmissible and still reached the same conclusion"[18] and that the interference was, therefore, unnecessary and excessive.
- In ***M.N. and others v. San Marino***, the Court set a few important understandings regarding the concept of private life and the application of Article 8. First, that professional or business activities can be included in the notion of "private life"[19]; second, that "all the exchanges in which individuals may engage for the purposes of communication"[20], including emails, are protected by the right to private and family life; third, that both the storing and the release of information concerning private life are protected by such right and that a refusal to allow an opportunity to refute such information amounts to an interference with the right to private life. Finally, the decision also analysed the matter of "necessity in a democratic society" under the lens of adequate measures against arbitrariness - "including the possibility of an effective control of the measure at issue".[21]

[16] ECHR. S. and Marper v. the United Kingdom https://rm.coe.int/168067d216.
[17] L.L. v. France, paragraph 43. https://www.globalhealthrights.org/wp-content/uploads/2018/05/CASE-OF-L.L.--FRANCE.pdf
[18] Idem, paragraph 46.
[19] ECHR, *M.N. and others v. San Marino*, paragraph 52, available from: http://hudoc.echr.coe.int/eng?i=001-155819.
[20] Idem, paragraph 52.
[21] Idem, paragraph 73.

A similar balancing test can be found on the IACtHR's decisions when an interference into private life is concerned. According to the Inter-American Court of Human Rights, in such cases, it is necessary to assess (1) whether an interference is provided by law; (2) whether it pursues a legitimate aim; and (3) whether it is suitable, necessary, and proportionate (in other words, if it meets the proportionality test).[22] One watershed case is that of ***Artavia Murillo y Otros v. Panama***, where a general prohibition by the State of *in vitro* fertilization was deemed in violation of the American Convention. Of particular interest is the analysis of necessity—where it was found that less restrictive alternatives existed to achieve similar aims—and the strict proportionality analysis - where particularly high standards were raised in light of the deeply intimate aspect of the right at issue.

Finally, at the HCR and the UN system in general there are various indications of growing adoption of the proportionality principle as a basis for judicial decision-making. Specifically, a series of General comments expressly cover the matter, such as General Comment 29 (States of emergency), 27 (Freedom of movement) and n. 34 (Freedoms of opinion and expression), the latter stating:

> Paragraph 3 (of Article 19) lays down specific conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be "provided by law"; they may only be imposed for one of the grounds set out in subparagraphs (a) and (b) of paragraph 3; and they must conform to the strict tests of necessity and proportionality.[23]

General comment 34 is of particular note, since in it the three aspects of the proportionality test are explicitly cited - restrictive measures must be "appropriate to achieve their protective function" (suitability); they must be the least intrusive instrument amongst those which might achieve the desired result" (necessity); and "they must be proportionate to the interest to be protected" (strict proportionality).

The right to privacy primarily evokes a notion of exclusion. From its Latin roots, *'privatus'* indicates what is set apart from what is public, what is personal; the earlier formulation of this right by Samuel Warren and Louis

[22] Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia), 30*(1), 77–96. https://doi.org/10.4067/S0718-09502017000100004

[23] United Nations. (2011). *General comment no. 34. Article 19: Freedoms of opinion and expression.* United Nations. https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf, paragraph 22.

Brandeis referred it to the 'right to be let alone'.[24] Thus, it was no wonder that the negative obligations derived from it were stressed at first, as in the mention that

> the sphere of privacy is characterized by being exempt from and immune to abusive and arbitrary invasion or attack by third parties or the public authorities" (IACtHR, ***Ituango Massacres v. Colombia***). Nonetheless, the urge to also provide the means of asserting the right to privacy also as positive obligations arouse from factors such as the pertinence of privacy as an enabler and the means to the fruition of other rights.

The right to privacy encompasses a swathe of capacities and other rights that contribute to the foundation and embodiment of personality and identity. This is clearly stated in the IACtHR's decision on the case of ***Fernández Ortega et al. v. Mexico***, stating that:

> [T]he Court has specified that, even though this provision is entitled "Right to Privacy" [Note: it is entitled Protection of Honor and Dignity in Spanish], its contents include, inter alia, **the protection of private life.** Moreover, **the concept of private life is a wide-ranging term, which cannot be defined exhaustively**, but includes, among other protected forums, **sexual life, and the right to establish and develop relationships with other human beings**.[25]

Thus, departing from mostly negative obligations related to being "let alone", a broader range of obligations can be enforced by judicial authorities and law operators. This broad range of obligations is reflected in international courts in key cases related to specific subjects, representing particular aspects of the right to private life. We will now move on to shortly describing and analysing a few of these cases to expand on the several ways in which this right may manifest.

In the above-mentioned case of the ***Ituango Massacres v. Colombia***, 2006, the Inter-American Court of Human Rights analysed, among other subjects, the matter of the inviolability of the home as an aspect of the

[24] Samuel Warren, Louis Brandeis. "The right to privacy", in: 4 Harvard Law Review 193 (1890).
[25] https://www.corteidh.or.cr/docs/casos/articulos/seriec_215_ing.pdf, p. 40.

right to private life enshrined in Article 11(2) of the American Convention on Human Rights (ACHR).

The case revolved around attacks perpetrated by paramilitary forces upon residents of the towns of La Granja and El Aro, in the Ituango region of Colombia. Among other kinds of violence, the forces burned down houses, which prompted the Court to bring about the application of ACHR's Article 11(2). The connection between the right to privacy and the protection of home and family life is explained in the following excerpt from the Court's decision:

> The Court considers that the sphere of privacy is characterized by being exempt from and immune to abusive and arbitrary invasion or attack by third parties or the public authorities. In this regard, an individual's home and private life are intrinsically connected, because the home is the space in which private life can evolve freely.[26]

The Court underlined that the matter goes beyond an interference in private property, since the home is "the place where [...] private life took place".[27] That is, by losing their houses, the people of Ituango effectively lost a part of the "sphere" of privacy that they could enjoy. This was reiterated by the Court with reference to similar decisions by the European Court of Human Rights — namely, ***Ayder v. Turkey, Bilgin v. Turkey and Selçuk*** and ***Asker v. Turkey***.

In ***Tristán Donoso v. Panamá***,[28] the IACtHR also extended the concept of private life to private communications held by two persons, revealing two aspects of the right to privacy as provided by the ACHR: the protection of honour and dignity (art. 11.1) and the protection of private life and correspondence (art. 11.2). It also touches upon the three-part test for legitimate interference with this right as practiced by the Court, a subject we will expand upon later on.

Thus, as seen from the cases commented, the protection of human dignity substantiated in the rights to privacy and private life extends to various specific protections: the protection of home, as the place where "private life" unfolds; communications, as the ability to hold private conversations;

[26] Idem, p. 86.
[27] https://www.corteidh.or.cr/docs/casos/articulos/seriec_148_ing.pdf, p. 87.
[28] *Tristán Donoso v. Panamá*, Loy. L.A. Int'l & Comp. L. Rev. 2014, vol. 36:1185, available from: https://iachr.lls.edu/sites/default/files/iachr/Cases/Tristan_Donoso_v_Panama/Tristan%20Donoso%20%20Panama.pdf, pp. 1195-1198.

the development of human relations, as the ability to choose with whom to form bonds and relations; control over one's body, bodily functions and sexual life, as sovereignty over one's choices; and maintenance of one's honour and reputation, as the ability to present oneself to society as one sees fit and control one's social manifestation.

Furthermore, the IACtHR's case law extends this protection even to other aspects not explicit in the text of the Convention,[29] such as the interception of telephone conversations - as shown in the ***Escher y Otros v. Brasil*** case. In fact, the decision created a "future-proof" understanding of the right to privacy, stating that the State should adapt its application to the current technological scenario:

> The informational fluidity that exists nowadays puts people's right to private life at a position of greater risk, due to the higher amount of new technological tools and their increasingly more frequent use. This progress, especially when dealing with telephone interceptions and recordings, should not mean that people are put in a vulnerable position before the State or private actors. Thus, the State must adopt a responsibility to adapt to the current times the traditional formulae of protection of private life.[30]

With this in mind, we can observe a certain conceptual elasticity of private life as a necessary means to the realization of human dignity, including aspects of physical and social identity, personal autonomy and development and the relations a person holds with others and their surroundings.[31]

This jurisprudential development is in line with European case law stemming from the ECtHR. Looking at the Council of Europe's Guidelines on Safeguarding Privacy in the Media,[32] we may find similar thematic pathways in the interpretation of the European Convention's Article 8. The document, concerned with the balance between freedom of expression and privacy rights in matters concerning the media, highlights cases where consideration was given to the aforementioned aspects of private life when in tension with the practice of journalism. As such, we may cite, for example, cases in which the following aspects of the right to

[29] Maqueo Ramírez, M. S., Moreno González, J., & Recio Gayo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de Derecho (Valdivia), 30*(1), 77–96. https://doi.org/10.4067/S0718-09502017000100004

[30] https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf, p. 36. (Free translation).

[31] Caso Artavia Murillo y Otros, paragraph 143. https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf, https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf

[32] Council of Europe. (2018). *Guidelines on Safeguarding Privacy in the Media.* 1–46. https://rm.coe.int/prems-guidelines-on-safeguarding-privacy-in-the-media-2018-/168090289b

privacy were considered on performing such balance, as regarding family life (***Flinkkilä and Others v. Finland***, ***Zvagulis v. Lithuania***), physical integrity and medical information (***Fürst-Pfeifer v. Austria***, ***Armonienė v. Lithuania***), and other similar cases where the HIV-positive status of a patient is publicly disclosed - violating not only privacy, but also harming public trust in the public health system; moral integrity (***Standard Verlags GmbH v. Austria (No.2)***) or the right to one's image (***Mgn Limited v. the United Kingdom***).

At this point, it is important to highlight that the move from a diminutive conceptualization of privacy as the right to be let alone to an expanded sphere of private life rooted in the realization of human dignity brings about a change to an increasing volume of positive obligations of the State, where more structures and institutions may be needed.

In ***Gaskin v. the United Kingdom***, this is made clear by the European Court's understanding that achieving proportionality predicates there being an "independent authority [who] finally decides whether access has to be granted".[33] In other words, there is an actual need for the state to put in place the necessary structures and institutions for the protection of rights. This will be expanded upon and made even clearer when we touch upon data protection rights, which involve many such obligations, from providing access to information to ensuring due process, guaranteeing control over personal data and stopping unauthorized disclosure of personal data… etc.

The characterization of private life as a long-reaching concept is but the first step in the analysis of its delicate balance with other rights — especially freedom of expression— and determining when an interference is lawful. In reaching this balance, various matters need to be weighed in, such as consideration for the public's right of access to information — which makes up in itself an aspect of the right to freedom of expression.[34] Regional systems manage this weighing with a balancing test, which also resembles the theoretical framework for limitations on freedom of expression proposed by the UN[35] and more or less explicitly applied in various Human Rights Courts decisions regarding other human rights. These will be expanded upon in the following sections.

[33] Gaskin v. the United Kingdom, paragraph 49. http://www.bailii.org/eu/cases/ECHR/1989/13.html
[34] United Nations. (2011). *General comment no. 34. Article 19: Freedoms of opinion and expression*. Geneva: United Nations.
[35] Idem.

3. The development of data protection regulation

The characterization of data protection as an autonomous right is an ongoing debate in international courts and scholarship. It stems from the fact that data protection, as a regulatory issue, arose in part from privacy regulations, norms and concerns and evolved into new sets of obligations of the State needed in order to provide control by the individuals of the information that concerns them, as well as the means to achieve that control —access to this information, confirmation of its existence, correction of improper data, etc.

However, data protection goes beyond privacy considerations. There might be relevant data protection issues where privacy considerations are null or a mere afterthought, since one deals with the individual's private sphere itself and the other with control over one's data manifestation. In essence, the line that binds both together, as was with the concepts of private life and privacy, is the realisation of human personality: both privacy and data protection are instrumental in allowing an individual to fully develop their personality.

Thus, it can be said that the right to data protection derives from the right to privacy[36] while holding at least two major distinctive characteristics from the former: first, it acts specifically on personal data, laying out conditions and limits to its processing, rather than considering privacy issues from a personal point of view. Second, as personal information processing today is rather ubiquitous, data protection is relevant in order to preserve a considerable array of rights and values, from self-determination to non-discrimination, and including freedom of expression as well.

In practice, personal data protection is enshrined as an autonomous right in numerous legislations—no less, the Charter of Fundamental Rights of the European Union (Article 8). It has also been, for example, recently recognized as such in a decision by the Brazilian Supreme Court.[37] Equally

[36] Doneda, Danilo. Da privacidade à proteção de dados pessoais. São Paulo: RT, 2021.
[37] Schertel Mendes, Laura; Iglesias Keller, Clara. A new milestone for data protection in Brazil. Internet Policy Review, 13 May 2020.

significant, personal data protection are being the subject of legislation in 69% of the countries in the Americas and 66% worldwide.[38] Similarly, the Indian Supreme Court recently upheld privacy as a fundamental right (***Justice K.S.Puttaswamy (Retd.) v. Union of India***) which catalysed discussions on an Indian Data Protection Bill[39] – still under discussion to this date.[40]

This sound normative presence has been spearheaded by a few developments in the subjects of privacy and data protection. From the landmark decision by the Federal Constitutional Court of Germany on the census law, where it was upheld that "fundamental right guarantees in principle the power of individuals to make their own decisions as regards the disclosure and use of their personal data [...] this right to 'informational self-determination'";[41] to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,[42] and the Council of Europe's Convention 108 and its Protocols;[43] to the European Union's General Data Protection Regulation (GDPR), data protection regulation has strengthened and become a solid body of knowledge and practice in the last few decades.

The evolution of data protection legislation is nearly a fact of the development of information and communication technologies and its effects on how people's information is used. While a first generation of such legislation was focused on the management of public databases of citizens' personal data, following legislation would stress the privacy rights that could be actually exercised by the citizenry, making up a second generation of data protection norms.

Afterwards, newer generations of data protection laws would focus on overcoming the challenges of providing individual choice and control in the face of omnipresent data-collecting structures put in place by disproportionate actors,[44] such as the State and large corporations and, more recently, in reducing risks and harms related to data processing.

[38] Data Protection and Privacy Legislation Worldwide | UNCTAD.

[39] 'Law in India' (*DLA Piper Global Data Protection Laws of the World*, 30 November 2021) https://www.dlapiperdataprotection.com/index.html?t=law&c=IN accessed 1 February 2022.

[40] Bhavna Sarma, 'Legal Status of Privacy Rights in India – A Comprehensive Analysis of Personal Data Protection Bill, 2019' (*CyberBRICS*, 2 December 2021) https://cyberbrics.info/legal-status-of-privacy-rights-in-india-a-comprehensive-analysis-of-personal-data-protection-bill-2019/ accessed 1 February 2022.

[41] Bröhmer, J., Hill, C., & Spitzkatz, M. (Eds.). (2012). 60 Years German Basic Law: The German Constitution and its Court. Landmark Decisions of the Federal Constitutional Court of Germany in the Area of Fundamental Rights (2nd ed.), Konrad-Adenauer Stiftung, p. 144.

[42] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD.

[43] Convention 108 and Protocols (coe.int).

[44] Mayer-Schönberger, Viktor. Generational development of data protection in Europe, in: Agre, Philip; Rotenberg, Marc. (org.). Technology and privacy: the new landscape. Cambridge: The MIT Press, 2001.

The rich data protection regulation scenario that has thus developed holds some aspects that are important for the judicial decision-maker. In essence, there is a selection of principles, concepts and rights that should be taken into account when measuring the balance of decisions of privacy and data protection rights in the face of other fundamental rights. These will be touched upon in the following sections.

3.1. Data protection as a projection of individual and social liberties in the Age of Information

The implementation of data protection in its most widespread aspect is nowadays represented in the European context by the General Data Protection Regulation (GDPR),[45] which has served as a basis and inspiration for much subsequent legislation worldwide. It is based on the idea that the data subject —the citizens— must be in control of their own data by means of a set of rights that need to be actively guaranteed, by both private or state actors when they use their data, as well as a body of principles that shape and impose limits to every personal data processing activity.

This kind of legislation is profoundly connected to the manifestation of the individual in digital environments or mediated by digital devices, where all actions are translated into and recorded as bits and bytes of (personal) data. Thus, the rights and principles are suited to such an environment, although, in general, personal data refers not only to digital data, but to data held on any kind of medium.

The most recent legislative efforts are also based on the understanding that those digital technologies are increasingly omnipresent and intermediate human experience, interaction and life. As such, a fundamental power and informational imbalance arises, where the users of these all-seeing systems are either not technically knowledgeable or powerful enough to claim their rights for themselves. Such informational asymmetry generates the need for active transparency and accountability obligations and stringent consent requirements in relation to products and services based on personal data.

[45] See more: the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) is the European Union law on data protection, built upon the former Directive 95/46/CE which dates back to 1996. https://eur-lex.europa.eu/eli/reg/2016/679/oj

A relevant starting point to understanding data protection is the shared body of principles that are generally recognized as the basis for data protection regulations. Although their exact naming and format varies from one jurisdiction to the other, these are:

- Purpose limitation: data processing activities should be tied to a specific purpose which is made known to the data subject beforehand.
- Minimization or necessity: no more data than that which is strictly necessary to realize this purpose should be processed.
- Transparency: a data subject must have knowledge and understanding of the collection and treatment of their data.
- Quality or accuracy: data on a subject should be precise and updated.
- Access: the data subject should be able to access their data.
- Security: data controllers should apply appropriate technical and organisational security.

These same principles take up various formats in different normative instruments. For example, the Inter-American Juridical Committee's declaration on Privacy and Data Protection[46] mentions "lawful and fair purposes", "accuracy of data", "access and correction", "limited use and retention", "duty of confidentiality", "protection and security" and "accountability", among other principles specific to that instrument. The EU's GDPR[47] uses similar terminology, with "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "storage limitation", "accuracy", "integrity and confidentiality" and "accountability".

Besides principles, there is a set of data subject rights that must be observed when conducting data processing activities. These also vary among jurisdictions but are generally specifications of the previously cited principles—means of realizing those principles in practice, such as the right of access and rectification; cancelation and opposition; the right to explanation regarding automated decision-making and others.

In Latin American data protection practice, these are referred to as "ARCO" rights, meaning *Acceso, Rectificación, Cancelación y Oposición* (access, rectification, cancellation and opposition). They are general categories

[46] 86th REGULAR SESSION (oas.org).
[47] GDPR, art. 5.

of rights that may be expanded upon by specific legislation. The GDPR, for example, dedicates a section of its third chapter, on the Rights of the data subject, to these rights. Convention 108 of the Council of Europe, in its original form, also deals basically with the same rights,[48] although its modernised version brings further specifications.[49]

Most recently, new rights that are being introduced are more related to the individual's strict control over his data than to privacy - such as the rights related to automated decision-making or even the rights of portability or interoperability.

New and innovative data-intensive technologies increasingly make up the interface between the individual and other entities – other individuals, governments, employers, companies etc. This expanding technological interface poses increasing risks to data protection and privacy, as well as freedom of expression and other rights, as various areas of human activity are mediated by data. One recent and relevant mention which illustrates this was the Indian Supreme Court's order to appoint an independent panel to look into allegations that spyware had been used to hack phones of politicians, activists and journalists.[50] Commenting the case, Chief Justice of India NV Ramana drew a clear connection between privacy and data protection rights and freedom of expression, stating that:

> This is of particular concern when it relates to the freedom of Press. Such a chilling effect on the freedom of speech is an assault on the vital public watchdog role of the Press […] Protection of journalistic sources is one of the basic conditions for the freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest.[51]

In such a situation, rights of privacy and data protection, freedom of expression and thought, journalistic freedom and, ultimately, the democratic process are intertwined. With data-driven processes making up a significant portion of an individual's activities, the development of personality itself depends on certain conditions determined by these technologies and how they are developed and implemented. Recent national decisions illustrate this, where the processing of personal data was a central element in:

[48] Convention 108, art. 8.

[49] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, art. 9.

[50] 'Pegasus Row: India's Top Court Orders Probe into Snooping Allegations' (*BBC News*, 27 October 2021) https://www.bbc.com/news/world-asia-india-59059489 accessed 1 February 2022.

[51] Satya Prakash, 'Supreme Court Flags "Chilling Effect" on Freedom of Speech' (*The Tribune India*, 28 October 2021) https://www.tribuneindia.com/news/nation/supreme-court-flags-chilling-effect-on-freedom-of-speech-330503 accessed 1 February 2022.

- Determining work relations (***Jeremy Lee v. Superior Wood,*** Australia, 2019): an employee was dismissed for refusing to provide biometric data. The country's Fair Work Commission held that, based on the Privacy Act of 1988, the employer's actions were harsh, unjust and unreasonable, since Lee was not adequately informed of the collection and use of his data, did not manage to give free and informed consent and the use of biometric identification was not strictly necessary.[52]
- Mediating interactions with the State and providing transparency to public affairs (***Saket v. Union of India***): in the case, the High Court of Bombay found the Ministry of Information and Broadcasting had violated the applicant's privacy by uploading his personal data to its website following an access to information request. The Court found that the publication of such data was unnecessary and exposed the applicant to harm, while also disincentivizing future applicants from filing applications under the Right to Information Act of 2005 due to fear of having personal data disclosed in a similar manner.[53]
- Access to justice and media reporting of judicial proceedings: the Bombay High Court published guidelines prohibiting media reporting of judgements under the Sexual Harassment of Women at the Workplace (Prevention, Prohibition and Redressal) Act, 2013, without the Court's permission. This prohibition also extends to "Both sides and all parties and advocates, as also witnesses", who are "forbidden from disclosing the contents of any order, judgment or filing to the media or publishing any such material in any mode or fashion by any means, including social media, without specific leave of the court".[54]
- Public identification schemes (***Nubian Rights Forum and others v. The Attorney General,*** Kenya, 2021): the High Court of Kenya recently declared as unconstitutional the country's National Integrated Identity Management System (NIIMS), a digital ID system. The Court stated that the program should have been preceded by a Data Protection Impact Assessment and that an appropriate legal framework to mitigate privacy and data protection risks should have been in place beforehand.[55]

[52] 'Jeremy Lee v. Superior Wood' (*Columbia Global Freedom of Expression*, 1 May 2019) https://globalfreedomofexpression.columbia.edu/cases/jeremy-lee-v-superior-wood/ accessed 1 February 2022.

[53] 'Saket v. Union of India' (*Columbia Global Freedom of Expression*, 5 November 2020) https://globalfreedomofexpression.columbia.edu/cases/saket-v-union-of-india/ accessed 1 February 2022.

[54] 'Bombay HC Bars Media Reporting, Public Disclosure of POSH Judgments Without Permission' (*The Wire*, 27 September 2021) https://thewire.in/law/bombay-hc-bars-media-reporting-public-disclosure-of-posh-judgments-without-permission accessed 1 February 2022.

[55] 'New Kenya High Court Judgment Sets Important Precedent for Digital ID Privacy Protections and Processes' (*Open Society Justice Initiative*, 15 October 2021) https://www.justiceinitiative.org/newsroom/new-kenya-high-court-judgment-sets-important-precedent-for-digital-id-privacy-protections-and-processes accessed 1 February 2022.

In regional bodies, many data protection rights cases have arisen recently and shed light upon the application of said principles and rights. In ECtHR case law, one might refer to the case of ***Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland***, which deals with the issue of compiling public domain data on a particular individual and whether this practice violates the protection of private life. In this case, the applicants made claim to their right of freedom of expression in regard to the publishing of tax information of 1.2 million natural persons in Finland. The data was originally publicly accessible, and the companies involved merely compiled and organised the information. Some crucial findings of the case are the idea that even publicly accessible data may be protected under the right to private life, and that the processing of publicly available data "in a manner or degree beyond that normally foreseeable" gives rise to private life considerations.[56]

The case is also of particular relevance since it was an instance where the right to freedom of expression was balanced in face of the right to private life. The applicants put forth the defence that their publishing of said information was protected by the journalistic derogation of freedom of expression. The Court, however, found that the prohibition issued by the Finnish Data Protection Board to forbid the applicants from publishing personal taxation data was legal, legitimate and necessary in the case.

The analysis of the Court followed similar steps to those previously explained, checking if a foreseeable and accessible law existed (the country's data privacy law) and whether the interference in freedom of expression was necessary in a democratic society. On this last point, the analysis revolved essentially around aspects of the information being publicized and the public interest around it.

To expand on this, it is useful to refer to the Council of Europe's Guidelines on Safeguarding Privacy in the Media,[57] where a complete framework for balancing privacy and freedom of expression is exposed. The document proposes an analysis based on the following aspects: first, an analysis of the information's contribution to a debate of general interest (public interest). Second, the role of the person concerned is considered —public figures,[58] for example, have a more permeable private life, since their actions have made them the objects of public interest. Third, the prior

[56] CASE OF SATAKUNNAN MARKKINAP RSSI OY AND SATAMEDIA OY v. FINLAND.pdf (columbia.edu), paragraph 136.

[57] Council of Europe. (2018). Guidelines on Safeguarding Privacy in the Media. 1–46. https://rm.coe.int/prems-guidelines-on-safeguarding-privacy-in-the-media-2018-/168090289b

[58] "Public figures are persons holding public office and/or using public resources and, more broadly speaking, people who play a role in public life", Council of Europe & Journalist Ethics Committee. (2012). Recommendations On The Protection Of Privacy In Media Coverage.

conduct of the person concerned is considered. Voluntary disclosure of information might reduce the degree of privacy protection afforded to a person; and fourth, both the method of obtaining information and its veracity are considered —journalists should use fair methods of obtaining information and strive for the veracity and quality of information provided to the public. This is a point that speaks especially to the analysis of public interest, since information of questionable quality logically contributes less to public debate.

Public figures, particularly politicians, people with incidence in public life or in a position of responsibility, still hold their privacy rights; however, some consideration must be given to the fact that they can attract attention and their position may limit in some cases their expectancy of privacy. Particularly relevant is the fact that some of their acts, as they may be subjected to public scrutiny, mustn't be covered by privacy rights or other means. See also HRC General Comment 34, par. 38.

Finally, consideration must be given to the content, form and consequences of publication. In this step, matters such as the publication of particularly sensitive information (home addresses and phone numbers, health data, children's identity), the reach of publication (local, national, regional, global etc.) and other context-specific matters are taken into consideration to weigh the benefit to public interest against the harm to private life.

It is important to note that the journalistic exemption figures in many modern data protection regulations. Thus, when journalists need to process, and even publish, personal data as part of their core activities, they might enjoy these exemptions and derogations. However, even so, much care should be taken not to cross the line between legitimate expression and abusive interference with privacy and data protection. The concept of public interest remains a relevant measure for that delicate analysis, as well as the framework previously described.

The issue of journalistic activities is but one of the areas where conflicts arise between privacy and other human rights. In any area where such conflicts arise, however, judicial actors may rely on the tools presented up to this point to mitigate issues and assess the balance of rights.

Conclusion and recommendations

1. The right to data protection is recent compared to freedom of expression rights and, as such, any evaluation about it should consider its presence in ongoing trials, debates and documents and also its instrumental nature as an enabler of other related human rights, besides its gradual yet constant evolving presence in human rights documents and statutes.

2. As information and communication technologies intensify the availability of information and its uses, the right to data protection and freedom of expression must more and more be mutually evaluated and considered. In this sense, cases which would be typically analysed according to freedom of expression standards may also increasingly demand the consideration of the data protection rights potentially (or actually) involved —and vice-versa.

3. The three-part test is an adequate and viable instrument to consider the interactions between data protection and freedom of expression rights and should be employed in order to keep them both substantial at their maximum extent.

4. The right to data protection and freedom of expression both evolved from technological innovation. Thus, the balancing of such rights should consider both the technological impact to them —in terms of risks and harms— as its eventual impact to the use of these technologies,[59] as the very possibility of exercising these rights is often provided by technologic features themselves.

[59] See more: The impact of the balancing on the technologies can be, by itself, substantially important to human rights, as in the example of the use of encryption technologies to communications: even considering the technical nature of encryption, opposed to, say, a normative nature, this technology can play a substantial role in the enforcement of the privacy of communications. See: UNESCO. Report on Human rights and encryption. Wolfgang Schulz, Joris van Hoboken. 2016, https://unesdoc.unesco.org/ark:/48223/pf0000246527

About these guidelines

The publication of the guidelines was made possible thanks to the support of the Open Society Foundations and the Multi-Donor Programme on Freedom of Expression and Safety of Journalists.

About the author

Danilo Doneda is a Brazilian lawyer and law professor at IDP with a Ph.D. in civil law from State University of Rio de Janeiro. He serves as a coordinator of the Centre for Internet, Law, and Society of IDP, a member of the National Data Protection and Privacy Council (CNPD) on behalf of Brazil's House of Representatives, a member of the Board of Directors of IAPP (International Association of Privacy Professionals) and a member of the advisory boards of the United Nations Global Pulse Privacy Group and the Project Children and Consumption (Instituto Alana). In the past, he served as general coordinator at the Department of Consumer Protection and Defense in the Ministry of Justice (Brazil). He was a former visiting researcher at the Italian Data Protection Authority (Rome, Italy), University of Camerino (Camerino, Italy), and the Max Planck Institute for Comparative and International Private Law (Hamburg, Germany). He has authored books and several papers and articles about civil law, privacy and data protection.

Published in 2022 by the United Nations Educational, Scientific and Cultural Organization, 7, place de Fontenoy, 75352 Paris 07 SP, France

CI-2022/FEJ/ME-1

Graphic and cover design: Estudio del Plata/Marcelo Falciani.

Printed by: UNESCO.

With the support of the
UNESCO Multi-Donor Programme on Freedom of Expression
and Safety of Journalists