# THE RIGHT TO PRIVACY AND PERSONAL DATA: SOME CONSIDERATIONS FOR OPTIMAL PROTECTION

**BY**
**BLANCA LILIA IBARRA CADENA**

President Commissioner of National Institute for Transparency, Access to Information and Personal Data Protection (INAI México), Chair authority of the Global Privacy Assembly.

Visit www.competitionpolicyinternational.com for access to these articles and more!

## THE RIGHT TO PRIVACY AND PERSONAL DATA: SOME CONSIDERATIONS FOR OPTIMAL PROTECTION

By Blanca Lilia Ibarra Cadena

The protection of privacy and personal data is a must for maintaining democracies and avoiding authoritarianism led by extreme surveillance. For the optimal protection of both rights, it is necessary to promote regulatory compliance, ethics, self-regulation, the strengthening of regulations, and of public bodies and institutions.

# 01
# INTRODUCTION

Privacy is the key to the most intimate details of our lives. We do not want to disclose certain information without our consent. In turn, privacy entails the protection of personal data. Safeguarding both rights is a must for maintaining liberal democracies and avoiding authoritarianism led by extreme surveillance from both private and public corporations.[2]

Personal data has acquired a high value in the current economic system. Such value "is not based on the data but rather on its management, use, and relationship to other data."[3] This situation has caused large and medium-sized technology companies to profit from the overuse of personal data to predict users' behavioral patterns.[4]

There has been a broad discussion about social media, disruptive technologies, and the ongoing surveillance we all experience. I would first like to state a clear stance: I am not against technology and innovation; on the contrary, I am in favor of progress. I am aware that technological advances form a key part of the development and progress in areas as critical as medicine and personal safety. In Mexico, many people use social media daily. For example, according to the 17th Study on Users' Internet Habits in Mexico, by the Internet Association MX ("AIMX"), in 2020, there were 84.1 million Internet users in Mexico, representing 72 percent of the population.[5] However, it is worth questioning how online services work, particularly in light of their surveillance over user habits, behaviors, and data. This should be done admitting that there are risks, and working to improve the protection of users' rights and freedoms.

Many have led us to believe that modernity and progress mean implementing disruptive technologies to automate everything. In contrast, the idea of progress implies both the enhancement and improvement of knowledge and the material advancement of humanity; it also implies moral evolution.[6] We can contribute to such development in all these aspects by guaranteeing people's fundamental rights and strengthening democratic institutions.

Scientific and technological innovation is critical for the State's development, provided it is ethical and aimed at a more equitable and just society.

Multiple news items have emerged in recent years concerning unethical practices engaged in by international corporations such as Cambridge Analytica. Recently, much public attention was focused on the statements by Frances Haugen (the Facebook whistleblower), who claimed that the company had promoted misinformation to gain economic benefits.[7] In addition, she reported an in-house study carried out by the company that confirms that the Instagram platform is harmful to children and adolescents because it exacerbates certain psychological conditions. Despite the above, we continue to use these platforms. We have become dependent on them and justify their use in the name of efficiency.

As you may recall, as early as 1890, in the United States, jurists Warren and Brandeis had already established criteria for the right to privacy in the face of technological advances. In 1973, the United States put in place the "Fair Information Practice Principles" ("FIPPs"). In 1970, European countries started enforcing personal data protection regulations, Germany being the pioneer in this regard. Moreover, various supranational instruments acknowledge the general principles in this area using varying approaches. The Universal Declaration of Human Rights of 1948 and the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data represent the first supranational instruments regulating the right to data protection. Subsequently, there was the Council of Europe Convention on the Protection of Individuals concerning Automated Processing of Personal Data of January 1981, among other instruments.

---

2 Vélis, Carissa. (2021) "*Privacidad es poder"* (Privacy is Power) p. 98.

3 Mendoza Enríquez, Olivia A. (2018). "*Marco jurídico de la PDP en las empresas de servicios establecidas en* México: *desafíos y cumplimiento"* {PDP "Legal Framework for service provider companies in Mexico: challenges and compliance"}. Revista IUS, volumen 12, no. 41, p. 269. Available at http://www.scielo.org.mx/scielo.php?pid=S1870-21472018000100267&script=sci_arttext (viewed on March 13, 2022).

4 *Ibíd*.

5 Asociación de Internet MX, *17° Estudio sobre los Hábitos de los Usuarios de Internet en* México 2021 (17th Study on the Users' Internet Habits in Mexico, *2021*). Available at: https://irp.cdn-website.com/81280eda/files/uploaded/17%C2%B0%20Estudio%20sobre%20los%20Ha%CC%81bitos%20de%20los%20Usuarios%20de%20Internet%20en%20Me%CC%81xico%202021%20v16%20Publica.pdf, viewed on March 13, 2022.

6 Castillo Aguirre, Jesús. "*La evolución histórica de la idea de progreso en el contexto del desarrollo regional*," (Historical evolution of progress under a regional development framework), p. 380, available at https://www.redalyc.org/pdf/2631/263141553047.pdf.

7 Interview for the "60 Minutes - TV Show" *60 minutes.* Available at https://youtu.be/_Lx5VmAdZSI.

The above examples show that the principles of privacy are not new. However, much has been written of late, criticizing the law for not being sufficient to protect the public from the dangers of technological advances. Nonetheless, we never ask ourselves if developers are up to the task of building new technologies for the good of modern societies while still respecting the rights and freedoms of individuals. Therefore, it is necessary to consider whether technological advances must comply with the principles that are - and were - already established in international recommendations and guidelines.

In the current context, it appears that neither legislation nor self-regulation have been capable of orienting the behavior of organizations towards respecting the rights to privacy and personal data protection ("PDP"). Thus, unethical decision-making has always been present, although it grew shortly after the creation of Google, the pioneer of surveillance capitalism.[8]

Despite the above, I believe it is possible to get back on the right track for technological and market development respecting privacy and PDP. To this end, it is crucial to make ethical decisions in the interest of the common good and to comply with the general principles governing the matter, and, in general, focus on respect for fundamental rights.

# 02

# REGULATORY COMPLIANCE, ETHICS, AND SELF-REGULATION: THE VIRTUOUS TRIANGLE

To ensure that organizations and governments conduct their actions focusing on respect for human rights, we should consider three issues: first, compliance with regulations, whether they come from national or international legislation, as these incorporate principles of our concern that are crucial for safeguarding the rights. Undoubtedly, we should add ethics (recently incorporated into certain formal legislation in terms of ethical compliance). As the last cornerstone of the virtuous triangle for developing new information and communication technologies that are functional and respectful of privacy and the right to PDP, we have the implementation of self-regulation mechanisms.

Below, I will explain each point of the so-called virtuous triangle for adequately protecting the rights to PDP and privacy.

**A. Regulatory Compliance**

Regulatory compliance refers to abiding by legislation or conventional frameworks, and it is by nature mandatory. In case of non-compliance by corporations, they should be declared illegal and penalized.

Rules are based on guiding principles, establishing duties and rights. Therefore, compliance is the minimum basis for an organization to operate under an established regime.

Companies and organizations must understand that principles of respect for privacy have been in effect since 1948 and are updated through legislation, conventions, and international guidelines. [9] A country that has agreed on the matter in data processing must likewise comply with such principles, even in the absence of sound regulations throughout the State.

Regarding the principles of PDP and privacy, specifically on technological development, I consider the principle of privacy by design and by default to be transcendental. Therefore, privacy must come first before implementing technologies, systems, and functions, and especially when implementing artificial intelligence, big data, and virtual reality. The same is true for business operations, physical architectures, and network infrastructure, which are becoming fundamental for companies and governments to automate processes and tasks.

According to the former Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian,[10] in broad terms, this principle consists of integrating the guarantee of privacy into the core of the technology or system architecture. In other words, it seeks to ensure that confidentiality is set up by default, which means that thorough prior planning is required.

The principle of privacy by design and by default is a way to integrate and comply with the general principles before technology implementation, a protectionist approach to fundamental rights, which, I reiterate, is what is needed today

In addition to the above, an instrument is vital, together with the principle of privacy by design and default, to achieve

8 Zuboff, Shoshana, *La era del capitalismo de la vigilancia*. (The Era of Surveillance Capitalism), México, Paidós, p. 23.

9 The Universal Declaration of Human Rights of 1948 refers only to respect for private life.

10 Cavoukian, Ann. Privacy by Design, The 7 Foundational Principles. Available at http://jpaulgibson.synology.me/ETHICS4EU-Brick-Smart-Pills-TeacherWebSite/SecondaryMaterial/pdfs/CavoukianETAL09.pdf. Viewed on March 15, 2022.

controlled technology development or intensive data processing. These are known as PDP Impact Assessments ("PDPIAs").

Under the EU General Data Protection Regulation (Article 35),[11] the person in charge of data processing must analyze PDPIAs in the light of new technologies. Their nature, scope, context, or purposes may pose a high risk to personal data owners. This duty must be fulfilled before data processing. Thus, in my opinion, these assessments document the implementation of the privacy principle by design and default.

**B. Ethics and Ethical Compliance**

Ethics refers to "a model of a person or community's virtuous life and lived values, embodied in their practices and institutions."[12] This behavior includes professional practice. In companies, we usually call it company philosophy and are the mission, vision, values, and objectives that give it meaning. Therefore, we can say that organizations have ethics.[13]

Ethics stem from good or bad behavior. In this sense, Fernando Navarro García, Director of the Ethics and Corporate Social Responsibility Study Institute (*Instituto de Estudios para la* Ética *y la Responsabilidad Social de las Organizaciones*), points out that "*ethics [help] to forge (good) character through prudent, mediated and reflected decision-making.*" Thus, it is crucial to ponder their consequences for organizations and their stakeholders.[14]

Ethical corporations build legitimate confidence and security in society. Thus, on this topic, we cannot overlook ethics.

> ***Ethics refers to "a model of a person or community's virtuous life and lived values, embodied in their practices and institutions***

Ethics must be demonstrated and reflected in commitments, although reinforced through actions. Currently, we have seen that rules control ethical compliance. For example, the main goal of EU Directive 2019/1939 on compliance is to set up a standardized legal framework for European Union countries. This framework will ensure protection and anonymity for employees and those reporting possible infringements, breaches, or fraudulent actions in organizations. To this end, companies must implement proper approaches and procedures for complaints.

I think this is excellent practice, although we should ask ourselves why something done purely out of free will, such as ethics, had to be regulated. Are corporations ethical?

Some best practices that are proper to point out for ethical compliance are the following:

- To develop Codes of Ethics.
- To set up Ethical Committees to discuss how to proceed and the decision-making process.
- To encourage the role of *compliance officers* (not only in the criminal field but in *compliance* in general).
- To set up complaint mechanisms due to unethical behaviors.
- To implement straightforward procedures for the anonymous file of complaints and use of mechanisms.

In this regard, compliance with PDP principles is closely related to ethics. Organizations should consider it a capital gain since this builds up trust and legitimacy among users in a win-win environment. It is by far more profitable to be an ethical company that proactively complies with regulation in the long run.

**C. Self-regulation**

Self-regulation refers to those rules of behavior not required by law but voluntarily self-imposed, which must be disclosed to act under these rules. In my opinion, it is a matter of consolidating or materializing the ethical decision-making process through reliable actions.

Therefore, self-regulatory mechanisms are the third pillar or cornerstone of the virtuous triangle to guarantee the

11 Regulation 2016/679 of the European Parliament and the Council of April 27, 2016. Available at https://www.boe.es/doue/2016/119/L00001-00088.pdf.

12 De Zan, Julio. "*Conceptos de 'ética' y moral*" (Concepts of ethics and principles), p. 22. Available at https://archivos.juridicas.unam.mx/www/bjv/libros/5/2228/4.pdf.

13 Navarro García, Fernando. *"El triunvirato entre* ética*, ley y compliance"* (Triumvirate among ethics, law, and compliance), European Journal compliance and news, p. 46. Available at http://www.aeaecompliance.com/images/documentos/revista5/j5navarro.pdf.

14 *Ibíd*.

right to privacy and PDP. Some self-regulatory mechanisms deserve special attention, such as certifications, to keep a respectful approach to crucial rights and freedoms. For example, the deployment of information security management systems includes specifications for assets containing personal data, such as ISO 27000 international standard, specifically 27701, and the implementation of codes of ethics for each sector, implementation of internal policies, and even the adoption of measures excluded from the Law for the sake of proactive compliance.

As an example of the above, in Mexico, under public sector legislation, regulated entities require a PDPIA "*when trying to enforce or amend public policies, programs, systems or IT platforms, electronic applications, or any other technology involving intensive or relevant processing of personal data. Likewise, assess the actual impacts concerning specific processing of personal data to identify and mitigate potential risks related to the principles, duties, and rights of data holders and the responsibilities of those in charge, as provided in the applicable regulation*."[15]

On the other hand, legislation covering the private sector does not require an EIPD. Still, it is considered a practical recommendation, and it is up to the entity to decide whether to put it in place or not. In the latter case, we are under a self-regulated system already set and proposed in the Law.

# 03

# STRENGTHENING OF INTERNATIONAL AND NATIONAL REGULATIONS UNDER A DEEP GLOBAL MARKETPLACE

The mismatch of domestic regulations is a significant challenge that started since the e-commerce boom. The *Global Privacy Assembly* ("GPA"),[16] in its Working Plan 2021-2023, set a priority strategy, which entails a global regulatory framework with high and clear standards consistent with PDP as digitalization moves at a swift pace.

The fact that rules have borders (unlike e-commerce or international data flow) causes disadvantages and legal uncertainty for personal data holders. They will rely on the practices of the company with whom they contracted goods or services and the legislation of the country where the company is based.

As the UK Information Commissioner, Elizabeth Denham, stated at the 43rd Global Privacy Assembly conference: "If, for example, a foreign company breaches its Law or of the country of the data holder and with whom it is doing business, or if there is a security breach, it would be highly complicated for regulatory agencies or PDP guarantors to work together due to issues of jurisdiction and legal systems."[17]

In the words of the former Commissioner, "*The result of all of the above is an international problem that may be costing trillions of dollars to worldwide economies.*" As she also points out, the meeting point of common standards and a better law structure can decrease the problem. However, we information commissioners cannot regulate, since we do not have legislative powers, although we can encourage and foster international discussion with legal bodies to reach consensus and improve our domestic regulations. PDPIA "

While there are no easy solutions, I think an approach to that meeting point lies in PDP and privacy principles. We are already working on the fundamental PDP principles to be accepted by the GPA State Membership. Still, the convergence process must speed up since we take a long time to respond, considering the transfer of personal data in the global data economy.

15 *Artículo 3, fracción XVI de la Ley General de PDP en Posesión de Sujetos Obligados*. (Article 3, section XVI – General Law of PDP owned by regulated entities).

16 *The GPI "…first named as the International Conference of Data Protection and Privacy Commissioners until the 41st Conference, has been the premier meeting place of the world's data protection and privacy regulators and enforcers. The Assembly has grown substantially, and its membership now extends across many parts of the world."* Available at: https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/ (viewed on March 15, 2022).

17 See https://globalprivacyassembly.org/solving-the-billion-dollar-question-how-do-we-build-on-the-foundations-of-convergence/ (viewed on March 14, 2022).

# 04

# STRENGTHENING OF PUBLIC BODIES THAT GUARANTEE PDP AND PRIVACY, AND PROMOTING THE CREATION OF PUBLIC CYBERSECURITY AGENCIES

It is undeniable that organizations, by its nature, are looking to increase their power and control people's behaviors as much as possible. The State must prevent such situations to ensure the personal welfare of individuals and preserve the legal structure and public nature of authority. To this end, we need specialized bodies and institutions.

The agencies, institutions, or public bodies responsible for protecting personal data have the mandate of protecting and safeguarding this fundamental right. Caring for their autonomy and promoting its strengthening is essential for democratic systems. Watching people's data and personal lives means safeguarding their dignity and independence. As Philosophy & Ethics professor Carissa Véliz from Oxford University says: "Only to the extent that we take care of such autonomy is that they can make independent decisions and exercise complete freedom."[18] Thus, privacy is power. If people are empowered, they can make better decisions geared towards strengthening democratic systems and living in full where they can properly enforce their rights and freedom.

Part of the great challenge for data protection and privacy guarantor agencies is to raise awareness among the population, inform them, and promote their rights in this area to control their data (strengthening informational self-determination) and protect themselves against possible privacy vulnerabilities.

I also believe it is vital that States invest in cybersecurity and promote the creation of public cybersecurity bodies.

The protection of information assets, including personal data, is indispensable in our society because there are many risks in the online and offline environment; cyber-attacks are from day to day and increasingly sophisticated.

For years now, but to a greater extent due to the COVID-19 pandemic, societies have been steeped in the digital world and increasingly dependent on technology. Even when it comes to critical infrastructures, such as supply chains, transportation, and financial transactions, fundamental rights such as education and utility services, among others, currently operate through digital technologies. Therefore, we need an entity that ensures the privacy and security of personal data and our integrity and property.

We have seen alarming cases where malware exploits vulnerabilities in medical scanning equipment to step in and modify information and make cancerous nodules appear on an X-ray where there are none.[19] Or vice versa, a cyber-attack that almost contaminated a dam in the State of Florida in the USA.[20]

According to the Cybersecurity Report 2020 called Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean,[21] "the economic damage from cyber-attacks could exceed 1 percent of some countries' gross domestic product ("GDP"). In the case of attacks on critical infrastructure, this figure could reach up to 6 percent of GDP."

Since 2012, the United Nations Human Rights Council has acknowledged that human rights must be guaranteed online and offline.[22] It called upon all States to bridge the digital divide and increase the use of information and communications technology to encourage the full enjoyment

18 Véliz Carissa, *Privacidad es poder* ("Privacy is Power"), p. 89.

19 See "Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists," available at https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/ (viewed on March 14, 2022).

20 *Ibid.*

21 *Banco Interamericano de Desarrollo, Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf*. (Interamerican Development Bank, Report-2020- Cybersecurity: Risks, Progress and the Way Forward in Latin America and the Caribbean), p. 10 (viewed on March 14, 2022).

22 "*Afirma que los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos*;" p. 4. ("Article 19 of the International Covenant on Civil and Political Rights states that the same rights available off-line must be likewise true on-line, specifically relative to freedom of speech, which must be enforced regardless of the means the user chooses). Available at: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf (viewed on March 14, 2022).

of human rights for all by fostering an enabling, safe, and secure online environment conducive to the participation of all.

Therefore, I think it is essential to promote the creation of public cybersecurity agencies or institutions. We need specialized personnel to reinforce the lines of action already in different sectors. For example, in México, there are regulations relative to obligations in cybersecurity, especially in personal data security and other sectors such as telecommunication networks. Thus, we need an entity to lead the cross-cutting policies in this area, develop digital confidence among citizens and organizations, raise awareness and provide education on the subject matter to protect our fundamental rights in the digital arena.

> ***Since 2012, the United Nations Human Rights Council has acknowledged that human rights must be guaranteed online and offline***

# CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY™ INTERNATIONAL