

Legal protection of the right to privacy in the digital era**Received date: 17/03/2025****Accepted date: 10/10/2025**

Sabah HAOUES*
University of Batna1
sabah.haoues@univ-batna.dz

Abstract:

Cybercrimes include hacking, spreading computer viruses, financial fraud, identity theft, insurance fraud, and disclosing private information such as emails, videos, photographs, and voice recordings without the victims' consent. These crimes endanger individual privacy and data security.

This article examines the legal protection of privacy rights in the digital era, highlighting threats like

hacking, identity theft, and data breaches.

It explores the relationship between privacy and security, data collection and sharing implications, and existing legal frameworks to protect individuals' privacy rights.

The article emphasizes the importance of understanding privacy as a fundamental human right and discusses various international and national laws that protect this right against cyber threats.

Keywords: Right to Privacy; Privacy and Security; Cybercrime; Breaches of Privacy; Data Protection Law.

Introduction:

Criminal offenders can easily access irretrievable information. Personal data can easily be formed because it involves an individual's information, ranging from age and race to ethnic group, nationality, gender, and beliefs, which may be religious or political. It also includes discriminatory and phobic medical background, psychological ailments, employment history, job title, job situation, years of service, and family ties. This information about an individual is considered personal information. When combined, it provides a deep and complete picture of a person's tangible and intangible matters.

The importance of this study lies in its contribution to our understanding of the consequences of tracking, collecting, storing, analyzing, sharing, and using data concerning the privacy and security of participants.

Study problem: The problem that is being studied is: What is the impact of cybercrimes on the right to privacy and data security in the digital era, and how do current legal protections address these issues?

Study methodology: To address this problem, we employed an

* - Corresponding author.

analytical approach in our analysis of relevant legal texts. Additionally, we utilized a descriptive approach to gain a comprehensive understanding of the study's subject. This approach also allowed us to detail its most significant aspects.

Study plan: The study was meticulously delineated into three discrete chapters. The initial chapter, entitled "Establishing the Right to Privacy," elucidates the foundational principles of this right. The subsequent chapter, "Cybercrimes and the Right to Privacy," expounds upon the implications of this right in the context of cybercrime. The final chapter, "Laws Protecting the Right to Privacy," explores the legal framework designed to safeguard this right.

Chapter I: Establishing the Right to Privacy

1- The Fundamental Human Right to Privacy:

Privacy is one of the most essential and fundamental civil rights. The right to privacy "establishes a certain necessity...for the individual(s)"⁽¹⁾.

It is included in international human rights agreements such as the 11th article of the 1969 American Convention on Human Rights⁽²⁾, the 8th article of the 1950 European Convention on Human Rights⁽³⁾, the 12th article of the 1948 Universal Declaration of Human Rights⁽⁴⁾, and the 17th article of the International Covenant on Civil and Political Rights of 1966⁽⁵⁾.

The following treaties also help: The 1989 Convention on the Rights of the Child⁽⁶⁾, the 7th Article of the EU Charter of Fundamental Rights⁽⁷⁾, the 22nd Article of the Convention on the Rights of Persons with Disabilities⁽⁸⁾, and the International Convention for the Protection of the Rights of All Migrant Workers and Their Families⁽⁹⁾.

The concept of privacy includes the right to be free from unwanted attention and the right to refuse to disclose personal information about one's beliefs, theories, similarities, and behavior⁽¹⁰⁾.

Because privacy indicates the ability to control private information, data privacy and privacy are two sides of the same coin.

2- The importance of privacy rights:

Privacy and additional civil rights are closely linked. The freedoms of belief, speech, religion, assembly, and association are likely made possible by solitude⁽¹¹⁾. The concepts of privacy and self-determination are innately connected. Article 20(1) of the 1981 African Charter on Human and Peoples' Rights makes this declaration: "All societies have

the right to life."This means they have definite and absolute self-determination. Additionally, everyone has the right to express their political preferences and develop philosophically and economically according to their chosen guidelines⁽¹²⁾.

Self-determination (or private autonomy) is a standard that requires the ability to act or make decisions independently. This concept combines the material and immaterial forms of the process. Similarly, solitude at the individual level requires fundamental independence and individual autonomy. This makes it possible for the public to live authentic lives because they have control over what information is accessible about the bureaucracy and what information is shared about the ruling class.

Another fundamental concept is human excellence, a term that is instead disputed⁽¹³⁾, which means "one's sense of self-value and the commitment to evolve and respect God and ensure the well-being of other nations," ⁽¹⁴⁾ and is further connected to individual solitude. Among the models of international law that address human dignity are the Universal Declaration of Human Rights (UDHR) of 1948, the International Covenant on Civil and Political Rights (ICCPR) of 1966, and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) of 1966⁽¹⁵⁾. The African Charter on Human and Peoples' Rights 1981, the United Nations Convention on the Rights of the Child 1989, the United Nations Declaration on the Elimination of All Forms of Racial Discrimination 1963 ⁽¹⁶⁾, and the United Nations Convention on the Elimination of All Forms of Discrimination Against Women 1979 ⁽¹⁷⁾ are also notable.

Similarly, the European Convention on Human Rights of 1950 does not explicitly include financial and public rights; rather, it focuses on civil rights⁽¹⁸⁾. As a fundamental idea, human dignity is written into many constitutions⁽¹⁹⁾.

Chapter II: Cybercrimes and the Right to Privacy

1- Examples of data breaches:

Cybercrime shatters privacy and can manifest in many ways, such as identity theft, banking fraud, virus creation, hacking, and debts against an individual's privacy, for example, in the form of cyberstalking, cyberbullying, and online harassment.

Lawful and unlawful practitioners alike recognize the value of data, thereby making it accessible both physically and virtually⁽²⁰⁾. For

example, data is a primary target for hackers due to its relevance in perpetrating various cybercrimes. This is usually the case because data is not well protected, making illegal access possible. The main causes of data breaches are insufficient system and data security, loss or theft of encrypted flash drives, laptops, or smartphones; uncontrolled access to a database; and inadvertent disclosure, release, or publication of data. Some famous cases of data breaches include:

The biometric dossier was not endangered throughout the attack, as was the case during the 2018 incident. However, the names, telephone numbers, email addresses, and IDs of the affected individuals were compromised. This is due in part to India's centralized national identity database, Aadhaar, which stores the biometric and demographic information of 1.2 billion Indians and is used to verify voters' identities for financial, public, and other services⁽²¹⁾.

In 2017, the property and land registry system in South Africa was breached, exposing the names, genders, salaries, employment history, ID numbers, phone numbers, and home addresses of approximately 30 million South Africans⁽²²⁾.

In 2013, over 3 billion consumers were affected when their identities, email addresses, and passwords (which were stored with weak encryption) were compromised, along with their birthdates⁽²³⁾.

More than 350 clients of the international consulting firm Deloitte had their usernames and identification information leaked due to an unprotected file within the company⁽²⁴⁾.

In 2016, he began supplying an online searchable database containing the sensitive personal information of over 49 million people in Turkey, including their ethnic ID, first name, last name, date of birth, place of birth, and even their residential address⁽²⁵⁾.

In 2016, over 55 million Filipino voters⁽²⁶⁾ had their personal and biometric information compromised when the Commission on Elections (COMELEC) website was hacked.

2- Legal statutes that reinforce the coverage of data breaches:

Some countries require data breach notifications, unlike nations such as Argentina, Belarus, Costa Rica, Egypt, Japan, Macau, Malaysia, Madagascar, Mauritius, Panama, Russia, Saudi Arabia, and many more that impose no such law. Other countries have specific regulations, such as the Philippines' Data Privacy Act of 2012⁽²⁷⁾, Qatar's Law No. 13 of 2016 regarding Personal Data Protection⁽²⁸⁾,

Indonesia's Regulation No. 82 of 2012 and its implementing regulation⁽²⁹⁾, and Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems⁽³⁰⁾. Angola and Serbia require data breach notifications only in the private sector. In Argentina, the obligation to notify people of breaches does not extend to agencies, but they must document all breaches in case of an audit or investigation.

Like all other laws, those concerning data breach notifications have enforcement mechanisms or restrictions within their scope regarding who is covered by them, what constitutes a breach, and which observances or disobedient acts warrant attention. According to these laws, institutions affected by a breach must notify affected individuals and other relevant parties.

These laws retroactively define, through litigation, who is supposed to provide notice, to whom it should be provided, and whether it should be provided. Regarding the GDPR, unauthorized access to systems and data must be reported within 72 hours after a user has interacted with the data (Article 33). Data processors must inform data controllers of any accidents within 72 hours, and data controllers must inform the applicable EU member state's supervising data protection authority within 72 hours of an accident.

Legislation concerning data breaches contains pertinent exclusions related to business motives linked to notification. According to General Data Protection Regulation Article 34, whether or not the breach is considered serious and whether it is necessary to inform the data subject depends on the gravity of the breach. In cases where it is determined that the breach is unlikely to result in damage to the relevant parties, some data breach notification regulations do not require such notification. Under other legislation, notice is served when a certain threshold is reached. Notifications required within 60 days of a breach in U.S. territories are regulated by the Health Insurance Portability and Accountability Act (HIPAA) ⁽³¹⁾. However, when the health information of over 500 people is breached, the media and the Office for Civil Rights of the Department of Health and Human Services must be notified within 60 days. No report to the media is required if it does not involve the personal health information of over 500 individuals. However, the Department of Health and Human Services Office for Civil Rights must be informed within 60 days or at the start of the next calendar year⁽³²⁾.

Data breach notification laws extend to some countries, such as Canada, Indonesia, and the United States. These countries also require organizations that deal with data to implement security measures to safeguard it or take action to validate the breach and mitigate damages to the affected organization.

Chapter III: Laws protecting the right to privacy

1- International conservation of the right to privacy:

Each person is entitled to privacy under international human rights treaties. For example, the European Court of Human Rights ruled that correspondence stored on a computer server⁽³³⁾ is disseminated via telephone, email, and the Internet and is preserved by Article 8(1) of the European Convention on Human Rights. Additionally, individual information is stored for periods that respect the user's privacy. Data violations depend on the context in which the data was captured, the method used the result of that method, and the processing of the data. *UK v. Marper*⁽³⁴⁾.

The Inter-American Court of Human Rights stated that information sent or received via the Internet and other digital media is preserved by Article 11 of the 1969 American Convention, as in the cases of *Tristán Donoso v. Panama* and *Estrella EN U v. Brazil*⁽³⁵⁾. Similarly, the 2014 Convention on Cyber Security and the Protection of Personal Data provided the right to the protection of personal data, as determined in Article 8 of the African Convention.

Furthermore, the right to privacy is included in the most basic human rights of the 2000 Charter of Fundamental Rights of the European Union and Article 16(1) of the 1957 Treaty establishing the European Economic Community, comparable to the Treaty of Rome.

Data safety refers to the processes of spreading, collecting, storing, analyzing, applying, and disseminating information. Limitations are outside the monitoring or use of data from a person or machine. ⁽³⁶⁾ "It is thinking, imagination, and even dreams." You create information not only about a person but also about his or her relatives and their lives. Cuts are activities that cause changes in someone's condition.

Additionally, both local and international institutions, as well as private organizations, can now modify, add new data, and search databases that contain specific information. Each nation controls the process of collecting, maintaining, and sharing information with the private sector differently. For example, in 2018, the combination of a

particular lock and a tracking record was investigated because public and private data processing increased and was erroneously investigated. As a result, some institutions needed their information, which caused a privacy safety deficit⁽³⁷⁾.

Whether countries can process personal data depends on how closely their rules align with European data protection rules. For example, section 60 of the 2012 Ghana Data Protection Act says that the Ghanaian government can use individual data from residents without a court order for national security reasons⁽³⁸⁾.

2- Regional conservation of the right to privacy:

As a right, privacy warrants local intervention to safeguard it. Data protection crosses borders and is therefore transnational. Examples include the 2014 African Union Convention on Cybersecurity and Personal Data Protection⁽³⁹⁾ and the ancillary data protection regulations within the Organization of the Economic Community of West African States⁽⁴⁰⁾.

The European Union's Data Protection Directive (Directive 1995/46/EC⁽⁴¹⁾) had several regional legal ramifications. The General Data Protection Regulation (GDPR) took effect on May 25, 2018, replacing Directive 1995/46/EC within the European Union. This legislation applies to the processing, storage, usage, and sharing of EU citizens' data, as well as that of other countries, private businesses outside the EU, and even those within the EU. One objective of the GDPR is to streamline enforcement regarding the safeguarding of personal information processing, storage, usage, and sharing by individuals in the digital space, as well as how apps, technologies, services, and online platforms exploit this information. Another objective of the GDPR is to enable the seamless movement of personal data across borders while upholding the right to privacy and unifying data protection legislation.

The GDPR provides guidelines for personal data, how it is treated, and the responsibilities and duties of those who control or process personal data. It also establishes consequences for breaches and requires the reporting of data breaches within 72 hours of the event.

The GDPR also imposes further responsibilities on both data controllers (entities that decide the "why" and "how" of data processing) and data processors (entities that work on the data according to techniques specified by the data controller).

Additionally, the General Data Protection Regulation (GDPR) enables individuals to challenge profiling practices and safeguards their rights as consumers. At the same time, companies processing data have security responsibilities and restrictions on data access, rectification, deletion, and other data processing functions. The GDPR also gives transparency to data controllers. The GDPR also empowers data protection authorities to facilitate cooperation and coordination in data processing and protection. Non-compliance with this rule has dire consequences.

According to the European Court of Justice, the GDPR applies to EU institutions that "have operations involving the processing of data, however minutely"⁽⁴²⁾. Such data is processed within the framework of certain EU treaties, which clarifies my initial point. Non-EU entities that process the personal data of EU citizens to provide products or services or to observe consumer behavior to analyze trends and forecast consumer behavior are also subject to the GDPR if they are within the EU and offer or market services to the Union.

National security objectives and actions performed under the Common Foreign and Security Policy of the EU are exempt from the scope of the General Data Protection Regulation (GDPR). Regulation (EC) No 45/2001, issued by the EU Parliament and the Council on December 18, 2000, establishes rules for protecting privacy within Community institutions and is therefore outside the GDPR's scope⁽⁴³⁾. The European Data Protection Supervisor (EDPS) oversees the European Parliament and the Council's Directive 2016/680 of April 27, 2016, which concerns the safeguards and protection of individuals about the processing of personal data by public authorities in the prevention, investigation, and prosecution of criminal offenses and the execution of judicial sanctions⁽⁴⁴⁾. This directive is also known as the "Police and Criminal Justice Data Protection Directive." Under this directive, the GDPR only applies to this data.

One unilateral international data protection arrangement is the Council of Europe Convention for the Protection of Individuals about Automatic Processing of Personal Data of 1981 (ETS No. 108). The 2001 Additional Protocol to the Convention for the Protection of Individuals about Automatic Processing of Personal Data is an optional protocol that aims to establish supervisory authorities to ensure data protection and privacy in cases of cross-border

information transfer. Further developments include the 1981 Convention for the Protection of Individuals about Automatic Processing of Personal Data (No. 223), the World Intellectual Property Organization (WIPO), and the European Communities (EC) 223/018. The convention was updated to "fulfill two action objectives: meet the challenges resulting from the use of new information and communication technologies, and strengthen the enforcement of the convention," as stated by the Council of Europe⁽⁴⁵⁾.

It is also followed by the public and private sectors in all countries, as well as international governmental organizations, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data⁽⁴⁶⁾.

3- National conservation of the right to privacy:

Private and state organizations often have different guidelines for data security. In the United States, data protection laws apply to only a limited range of data types, such as financial, health, children's, and educational information that businesses create, store, analyze, and publish. Furthermore, the level of data security often varies depending on the type of data. For example, the content of an email is generally considered safer than the email addresses of the sender or recipient. The nature of the data (whether it is sensitive, offline, online, or sector-specific) along with its source can influence applicable data security laws, particularly concerning adults and minors.

In Mexico, there are two main data protection laws: the Federal Law on the Conservation of Personal Data, which governs the private sector and was enacted in 2010, and the General Law on the Protection of Personal Data, aimed at the public sector, which was established in 2017.

Additionally, Mexico has laws that address the preservation of personal information stored in the cloud, such as Skydata, which also covers the handling of user data once it is no longer available on the platform.

Conclusion:

Data plays a pivotal role in the landscape of cybercrime, a reality that becomes increasingly pressing in our technologically advanced era. While data holds immense potential for empowering individuals, businesses, organizations, and governmental entities, it is equally susceptible to misuse by certain malicious actors for illegal activities.

The concept of privacy has long been enshrined as a fundamental human right, a principle underscored in the Universal Declaration of Human Rights and various other international treaties focusing on civil and political liberties. This discourse delves into the realm of international laws governing privacy and data protection, crucial for comprehending how various international, regional, and national frameworks address these essential rights. We examine the intricate relationship between human rights and privacy, particularly in the context of the burgeoning field of artificial intelligence, thus offering a comprehensive exploration of this critical subject.

*In summary, we draw attention to the following **significant observations**:*

1. The notions of privacy, data security, and the security of systems and networks are profoundly interconnected and must be understood as a cohesive framework.

2. The processes involved in the collection, analysis, and transfer of data often outpace the preparedness of governments and organizations, leading to a plethora of cybersecurity vulnerabilities.

3. Numerous crimes committed online are largely enabled by how data is accumulated, stored, examined, and disseminated across different platforms and entities.

4. There is a prevalent issue of data distribution without obtaining proper consent from users, coupled with a lack of transparent alternatives for individuals regarding how their information is handled.

5. The existing legal frameworks and security protocols are frequently inadequate, falling short of addressing the challenges posed by evolving cyber threats.

*In light of these observations, we propose the following **actionable recommendations**:*

1. Enhance the robustness of security practices to effectively shield against cybercrime, ensuring the sanctity of data integrity and protecting users' privacy against unauthorized access and exploitation.

2. Fortify legal structures that safeguard data and personal information within the digital sphere, ensuring that there are stringent penalties for breaches and violations.

3. Develop and apply advanced protective measures in the online environment, drawing on the knowledge and expertise of countries leading the way in data protection and cybersecurity protocols.

4. Implement comprehensive educational initiatives aimed at raising awareness among individuals about safeguarding their personal information and equipping them with the tools necessary to prevent unauthorized data collection and utilization.

Referrals and References:

- ⁽¹⁾- *La protection internationale des droits de l'homme dans le cadre européen. Travaux du colloque organisé par la Faculté de droit et des sciences politiques et économiques de Strasbourg en liaison avec la Direction des droits de l'homme du Conseil de l'Europe, 14-15 novembre 1960, Librairie Dalloz, 1961, p. 67.*
- ⁽²⁾- *The American Convention on Human Rights was adopted by many countries in November 1969. It came into force on July 18, 1978, after the eleventh instrument of ratification (Grenada's) was deposited.*
- ⁽³⁾- *The European Convention on Human Rights was signed in Rome on November 4, 1950, and entered into force on September 3, 1953.*
- ⁽⁴⁾- *The Universal Declaration of Human Rights was adopted on December 10, 1948.*
- ⁽⁵⁾- *International Covenant on Economic, Social and Cultural Rights. United Nations Treaty Series, vol. 993, p. 3, December 16, 1966.*
- ⁽⁶⁾- *Adopted in 1989, and entered into force the following year.*
- ⁽⁷⁾- *European Union Charter of Fundamental Rights, The Charter was declared in 2000 and came into force in December 2009 along with the Treaty of Lisbon.*
- ⁽⁸⁾- *The Optional Protocol to the Convention on the Rights of Persons with Disabilities (A/RES/61/106) was adopted on 13 December 2006 at the United Nations Headquarters in New York and was opened for signature on 30 March 2007.*
- ⁽⁹⁾- *International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families, Article 14, Adopted by General Assembly Resolution 45/158, December 18, 1990.*
- ⁽¹⁰⁾- *Koops Bert-Jaap, and all: A typology of privacy. University of Pennsylvania Journal of International Law, (2017), Vol. 38(2), p 490.*
- ⁽¹¹⁾- *The United Nations High Commissioner for Human Rights Report on the right to privacy in the digital age. A/HRC/39/29.*
- ⁽¹²⁾- *African Charter on Human and Peoples' Rights, adopted June 27, 1981, entered into force Oct. 21, 1986*
- ⁽¹³⁾- *Philippe-André Rodriguez: Human dignity as an essentially contested concept. Cambridge Review of International Affairs, 2015, Vol. 28(4), p750.*
- ⁽¹⁴⁾- *Schroeder Doris: How to define dignity and its place in human rights- a philosopher's view. 2017, p69.*
- ⁽¹⁵⁾- *UN General Assembly, International Covenant on Economic, Social and Cultural Rights, United Nations, Treaty Series, vol. 993, p. 3, 16 December 1966,*
- ⁽¹⁶⁾- *United Nations Declaration on the Elimination of All Forms of Racial Discrimination, A/RES/1904, UN General Assembly, 20 November 1963.*
- ⁽¹⁷⁾- *Convention on the Elimination of All Forms of Discrimination against Women New York, 18 December 1979, Entry into force: 3 September 1981.*
- ⁽¹⁸⁾- *Pretty v. United Kingdom (App 2346/02) [2002] ECHR 423.*
- ⁽¹⁹⁾- *Shulztiner & Carmi: Human Dignity in National Constitutions: Functions, Promises and Dangers. The American Journal of Comparative Law, 2014, p 461-490.*

⁽²⁰⁾- Graham & Smith: *Cybercriminology, Cybercrime, and Digital Deviance*, 2019, p80.

⁽²¹⁾- Personal data of a billion Indians sold online for £6, report claims. *The Guardian*, 4 January, 2018. <https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar>. accessed 2^{ed} february2025.

⁽²²⁾- Top real estate company admits to being unwitting source of country's largest personal data breach. *Sunday Times*, 18 October 2017. at <https://www.timeslive.co.za/news/south-africa/2017-10-18-top-real-estate-company-admits-to-being-unwitting-source-of-countrys-largest-personal-data-breach/>. accessed 2^{ed} february2025.

⁽²³⁾- Yahoo's 2013 Email Hack Compromised Three Billion Account., 3 October 2017. At <https://www.wired.com/story/yahoo-breach-three-billion-accounts/> accessed 2^{ed} february2025.

⁽²⁴⁾- Deloitte hack hit a server containing emails from across the US government. *The Guardian*, 10 October 2017. at <https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government> accessed 5th march2025.

⁽²⁵⁾- Hack Brief: Turkey Breach Spills Info on More Than Half Its Citizens, 5 April 2016, at <https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/>, accessed 2^{ed} February 2025.

⁽²⁶⁾- Website claims: Registered voters' sensitive data easily searchable, 55M Filipino voters open to fraud after Comelec hack- int'l tech security firm. *CNN Philippines*, 8 April 2016. at <https://www.cnnphilippines.com/news/2016/04/21/Comelec-hack-data-registered-Filipino-voters.html>, accessed 2^{ed} february2025.

⁽²⁷⁾-The Data Privacy Act of 2012 ("Act" or "DPA") or Republic Act No. 10173, which took effect on 8 September 2012, is the governing law on data privacy matters in the Philippines.

⁽²⁸⁾-Qatar. Law No. (13) Enacting the Privacy Protection of Personal Information Law (2016)

⁽²⁹⁾-Gov. Reg. PP 82/2012 Electronic system and transaction operation; at http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4902_PP_82_2012_e.html, accessed 7th February 2025.

⁽³⁰⁾-Data Protection Laws and Regulations Report 2024 Indonesia; at <https://iclg.com/practice-areas/data-protection-laws-and-regulations/indonesia>, accessed 4^{ed} february2025.

⁽³¹⁾-Health Insurance Portability and Accountability Act of 1996 (HIPAA) | Public Health Law, United States of America, 1996.

⁽³²⁾- Summary of the HIPAA breach notification requirement, *HIPAA Journal*, 2015.

⁽³³⁾-Wieser And Bicos Beteiligungen Gmbh V. Austria- Rezolucja Komitetu Ministrów Rady Europy , at <https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/74336-01-wieser-and-bicos-beteiligungen-gmbh-v-austria-521918690>, accessed 2^{ed} february2025.

⁽³⁴⁾-S. And Marper V. The United Kingdom, 4 December 2008, at <https://www.bailii.org/eu/cases/ECHR/2008/1581.html>, accessed 2^{ed} February 2025.

⁽³⁵⁾-Inter-American Court of Human Rights: Case of Escher and ors v Brazil, José Escher and ors v Brazil, Preliminary objections, merits, reparations, and costs, 6th

July 2009, at https://opil.ouplaw.com/view/10.1093/law-ihrl/4111_iachr09.case.1/law-ihrl-4111iachr09. accessed 2^{ed} february2025.

⁽³⁶⁾- Paul Bernal: Data gathering, surveillance, and human rights: recasting the debate. *Journal of Cyber Policy*, Vol. 1(2), 2016, p 243-264.

⁽³⁷⁾-General Assembly, Human Rights Council, Resolution (A/HRC/RES/34/7)

⁽³⁸⁾- The Data Protection Act of 2012 in Ghana is an act that establishes a Data Protection Commission to protect the privacy of individuals and their data. It does so by regulating the processing of personal information and providing processes for obtaining, holding, using, or disclosing personal information. The date of assent is May 10, 2012.

⁽³⁹⁾- African Union Convention on Cybersecurity and Personal Data Protection, 2014

⁽⁴⁰⁾-Economic Community of West African States (ECOWAS) Personal Data Protection A/SA.1/01/10, at <https://www.ecowas.int/member-states-experts-validate-the-revised-supplementary-act-a-sa-1-01-10-on-personal-data-protection-within-ecowas/>, accessed 25th January 2025.

⁽⁴¹⁾-the European Parliament and Council released Directive 95/46/EC, which addresses the protection of individuals about the processing of personal data and its unfettered transfer, On October 24, 1995.

⁽⁴²⁾-Weltimmo v. Hungarian Data Protection Authority, Case C-230/14, 30 October2015.at<https://eur-lex.europa.eu/legal-content/>.accessed 4th January 2025.

⁽⁴³⁾- European Parliament and Council Regulation (EC) No 45/2001 of December 18, 2000, on the protection of individuals concerning the processing of personal data by Community institutions and bodies and on the free movement of such data; available at <https://www.legislation.gov.uk/eur/2001/45/chapter/V> accessed 2^{ed} February 2025.

⁽⁴⁴⁾-The European Union Agency for Fundamental Rights posted Directive (EU) 2016/680 of the European Parliament and the Council on April 27, 2016, on the protection of natural persons through the processing of personal data by competent authorities for prevention, investigation, detection, etc. at

<https://fra.europa.eu/en/law-reference/directive-eu-2016680-European-parliament-and-council-27-april-2016-protection-natural>, accessed 10th march 2025.

⁽⁴⁵⁾-The 1981 Convention for the Protection of Individuals concerning the Automatic Processing of Individual Data is available at <https://www.refworld.org/legal/agreements/coe/1981/en/31908>. accessed 2^{ed} february2025.

⁽⁴⁶⁾-Guidelines for Safeguarding Privacy and Transnational Personal Data; At https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en. accessed 3^{ed} march 2025.