25th International Marketing Trends *Conference*
16-17 January 2026, Berlin-Germany

Digital footprint of internet users, what about security and data protection challenges? An examination in the North-South context

Augustin MBAM, Université de Picardie Jules Verne, augustin.mbam@u-picardie.fr

Abstract:
The digital footprint of internet users, a reflection of their online activities, has become a major strategic issue in digital governance. Despite notable legislative efforts, the rise in cyberattacks in both France and Cameroon reveals persistent weaknesses in the protection of personal data. These vulnerabilities stem from technological, legal, economic, and sociocultural disparities. In France, the GDPR provides an advanced legal framework but must evolve to address challenges posed by emerging technologies such as AI, Blockchain, IoT, and the Metaverse. In Cameroon, although laws exist, their implementation remains limited and requires adaptation to local realities. In response to these challenges, we identify three key areas for action: (1) strengthening legal frameworks and adapting them to technological developments, (2) fostering North-South international cooperation, including information sharing, the creation of a Cybersecurity Criminal Court, and skills transfer for a global approach to cyber threats, and (3) promoting accountability among organizations and individuals through education, awareness, and the adoption of good digital practices. These strategies aim to build a more ethical, inclusive, and sustainable digital space, where data protection is seen as a fundamental right rather than a luxury.

Keywords: Digital Footprint; Consumer; Security; Data Protection; North-South Context.

Digital footprint of internet users, what about security and data protection challenges? An examination in the North-South context

Introduction

Globalization has truly transformed the planet into a "global village". Driven by information and communication technologies (ICT), interactions between individuals and organizations now transcend borders at lightning speed, reshaping how we communicate, work, and live—while leaving behind a vast trail of digital footprints. In 2023, 66% of the global population was connected to the Internet, with a penetration rate of 87% in Europe compared to around 40% in many African countries, and an annual growth of over 20% in the number of internet users (ITU, 2023). By early 2024, social media users reached 5.04 billion, representing 62.3% of humanity (Statista, 2024). The Digital Report 2025 estimates the total number of internet users at 5.56 billion, up 2.5% year-on-year, and suggests they spend an average of 6 hours and 38 minutes online daily. The Global Internet Phenomena Report 2024[1] confirms that video streaming (Netflix, YouTube, Amazon Prime Video, etc.) accounts for more than 80% of global internet traffic. In 2024[2], over 250 billion apps were downloaded by users[3]; 4.37 billion people used email[4], while instant messaging apps had over 3 billion active users[5], and approximately 361.6 billion emails circulated daily worldwide[6]. Every online activity generates digital traces, many of which contain sensitive and personal information. Despite regulatory frameworks such as the California Consumer Privacy Act (CCPA – United States), the General Data Protection Regulation (GDPR – Europe), and the Malabo Convention on cybersecurity and personal data protection (Africa), vulnerabilities persist and data breaches continue to multiply.

The caution displayed by internet users has not prevented major scandals. According to INSEE[7] (2021), 82% of internet users reported taking measures to protect their personal data, yet the year 2021[8] revealed the fragility of these safeguards: a major data breach affected Facebook, exposing the personal information of over 500 million users. This leak hit European users particularly hard, calling into question the effectiveness of GDPR protections (European Commission, 2018). The exposed data included phone numbers, Facebook IDs, full names, places of residence, birth dates, and email addresses. In France, the situation was especially striking: out of 40 million Facebook subscribers, nearly 20 million—one in two users—had their data compromised. "*It would not be surprising if hackers exploited the stolen data to launch targeted phishing campaigns [...]. It is also likely that cybercriminals will use this information to impersonate the hacked individuals,*" explained Dimitry

---

[1] https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2024/GIPR/GIPR%202024.pdf

[2] https://startups-nation.fr/mediametrie-2024-une-annee-record-pour-l-usage-dinternet-en-france/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

[3] People who, at least once during a given reference period, accessed the Internet via any device (computer, mobile phone, console, connected television, etc.), regardless of the location of connection (home, work, educational institution, public space or mobile network) (ITU, 2020).

[4] https://independant.io/statistiques-emailing/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

[5] https://www.ecommerce-nation.fr/e-commerce-video-reseaux-sociaux-chiffres-internet-francais-2024/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

[6] https://independant.io/statistiques-emailing/?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

[7] https://www.insee.fr/fr/statistiques/6475020?t&citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

[8] https://www.20minutes.fr/high-tech/3015963-20210407-facebook-tout-comprendre-fuite-donnees-concerne-533-millions-utilisateurs

Galov, a security expert at Kaspersky. The trend has not reversed since: in 2024[9], phishing attacks and data breaches increased by 23% in Europe.

The CNIL[10] recorded 5,629 incidents in one year—a 20% increase—including major data breaches involving "France Travail" and the telecom operator "Free," which compromised the personal information of over one million individuals. Despite the strict standards imposed by the GDPR to ensure the security and protection of personal data, these incidents highlight the resurgence and escalation of digital attacks.

In contrast, within the African context, the digital revolution is progressing faster than legislation. Regulatory frameworks often remain embryonic or under development, exposing internet users to heightened risks of data breaches and cybercrime (Interpol, 2022). Inspired by the European GDPR, countries such as South Africa, Benin, Cameroon, Morocco, Nigeria, and Senegal have adopted tailored legal instruments that complement the 2014 Malabo Convention. In Cameroon, for instance, Law No. 2024/017 of December 23, 2024[11], establishes key principles for data protection and imposes specific obligations on businesses and public administrations.

However, the implementation of these standards remains unclear in many states, and 17 out of 54 African countries[12] still lack any specific legal instrument to date. These include Chad, Guinea-Bissau, Eritrea, Somalia, South Sudan, the Central African Republic, Sierra Leone, and Libya. This regulatory vacuum may help explain the proliferation of cybercrime, including a surge in ransomware attacks and online scams. According to Interpol's 2023[13] report, more than 10,490 cybercrime-related arrests were made across 19 African countries. Recently[14], South African telecom operator MTN Group disclosed a breach that allowed an unidentified third party to access customer data, though the extent of the leak was not specified.

Although detailed data on specific incidents is not always publicly available, these vulnerabilities are enough to significantly erode user trust and place a heavy burden on businesses. According to a 2024 analysis by Secureframe[15], 94% of companies believe their customers would not do business with them if they failed to adequately protect personal data. Yet only 20% of data protection professionals report full confidence in their organization's compliance. Furthermore, Cybersecurity Ventures[16] estimates global losses from cyberattacks at $6 trillion in 2021, up from $3 trillion in 2015. These findings illustrate the growing scale of threats to internet users' data and the complexity of the challenges faced by organizations—particularly in a context where protection levels vary widely across regions, with stricter regulations in Europe (GDPR) and more flexible, vague, or nonexistent frameworks in certain Southern countries.

Unexplored Questions in the Literature – Research Gap

---

9 https://www.interpol.int/fr/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_FR%20v3.pdf

10 https://www.cnil.fr/fr/violations-massives-de-donnees-en-2024-quels-sont-les-principaux-enseignements-mesures-a-prendre?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

11 https://prc.cm/fr/actualites/actes/lois/7588-loi-n-2024-017-du-23-decembre-2024-981daa162054

12 https://cybersecuritymag.africa/etats-des-lieux-des-legislations-sur-protection-donnees-personnelles-afrique?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

13 https://www.enqueteplus.com/content/rapport-mondial-2024-d%E2%80%99interpol-sur-les-cybermenaces-en-afrique-le-nouveau-cancer-du?citationMarker=43dcd9a7-70db-4a1f-b0ae-981daa162054

14 https://blog.infrascan.net/2025/04/25/une-cyberattaque-chez-mtn-expose-les-donnees-de-clients-africains-dans-plusieurs-regions/

15 https://secureframe.com/fr-fr/blog/data-privacy-statistics

16 https://cybersecurityventures.com/annual-cybercrime-report-2020/

The digital footprint of internet users is a central concept in the global digital ecosystem, referring to the traces left during online activity—whether voluntarily (posts, comments) or involuntarily (cookies, metadata) recorded (Clarke, 2014; Clarke, 2019). These traces are exploited for commercial, security, and political purposes, raising significant concerns regarding personal data protection (Maciel-Hibbard, 2018). However, the analysis of data security and protection issues remains limited at the global level, and within a North–South context, it raises complex questions related to legislation, technology, and sociocultural perceptions of privacy.

The European Union, particularly through the General Data Protection Regulation (GDPR), is frequently cited as a model (Walczak, 2014), and some countries in the Global South occasionally draw inspiration from these standards. However, they often lack the necessary infrastructure for effective implementation, resulting in a form of protection that remains largely theoretical (Maciel-Hibbard, 2018). The massive collection of personal data (Solove, 2006; Zuboff, 2019) exposes users to risks such as surveillance, manipulation, and identity theft. In Southern countries, these risks are exacerbated by the lack of secure infrastructure. Moreover, inequalities in access to information and digital education make these populations more vulnerable to the abusive exploitation of their data (Couldry et Mejias, 2019). The absence of appropriate structures complicates the implementation of effective protection mechanisms, especially since perceptions of privacy vary significantly between the North and the South, influencing both the design and effectiveness of data security strategies (Nissenbaum, 2009). However, research that integrates these sociocultural dimensions remains scarce, particularly within a comparative North–South framework. Most studies focus on Western countries, overlooking the specificities of developing nations (Milan et Treré, 2020). These gaps limit the global applicability of data security and protection strategies. Furthermore, the responsibility of public and private actors (institutions, companies, NGOs, etc.) in educating and raising awareness among individuals also requires particular attention, especially in countries where regulations are less stringent.

It is therefore essential to rethink approaches to personal data protection in order to address emerging digital threats. The vulnerability of internet users in both regions raises critical issues regarding digital trust, respect for privacy, and the sustainable development of digital ecosystems. This paper thus seeks to explore how certain mechanisms—legal, technological, or sociocultural—can be mobilized to meet these challenges in both France and Cameroon. To do so, we adopt a transdisciplinary approach, combining law, sociology, management, and technology to formulate a set of actionable strategies to overcome these challenges. These strategies will be preceded by a situational analysis of online data security and protection in both France and Cameroon.

I. State of play of security and protection of personal data online in France and Cameroon

Digital footprints, which encompass personal data, consumer habits, and user preferences, have become a key strategic lever for businesses. However, they raise growing concerns about information security and protection, as users are often unaware of the dangers associated with the collection and use of their data.

Despite legislative efforts and other measures put in place to ensure the security of ICT use, there has been a resurgence of cyberattacks in both France and Cameroon, as well as a worrying increase in online personal data breaches, thus revealing flaws in digital governance systems in both France and Cameroon.

1. The persistence and growth of digital attacks

Cyberattacks are experiencing significant growth in both France and Cameroon, largely due to technical and organizational flaws that provide leverage for cybercriminals. It is also crucial to emphasize that legal gaps hamper an appropriate response to certain types of attacks.

1.1 Technical and organizational flaws

Looking at the trends of the last 5 years in France, from 2019 to 2023, we see a 40% increase in digital offenses, which represents an annual increase of 8%[17]. Various factors explain this situation, including technical and organizational flaws. These flaws include software vulnerabilities, ransomware attacks, and social engineering techniques[18]. As for organizational failures, these result largely from a lack of awareness and retraining of employees, particularly those working remotely, who represent the main gateway to these attacks[19]. In addition, delays in updating IT systems within companies significantly increase the risk of attacks. According to the CESIN barometer, in 2024, 40% of French companies were carrying out late updates.

Furthermore, the often-insufficient budget allocated to cybersecurity limits the acquisition of advanced protective equipment, thus exposing users, including businesses, to permanent threats[20]. Cameroon, in the midst of a digital transformation, the situation is worrying, with a worrying increase in cyberattacks targeting administrations, businesses and individuals. The main attacks reported between 2023 and 2025 include ransomware attacks, mainly targeting banks and Fintechs[21], as well as other threats such as massive data leaks, phishing, online fraud, fake wire transfer orders[22], telephone scams, identity theft, and fake profiles on social networks (including romance scams and blackmail). Clearly, we can emphasize that France is equipped to respond to the computer threats it is a victim of every day, but the existing framework for combating them unfortunately seems insufficient to contain the growth of cyberattacks that are reinvented every day in the country. Cameroon, for its part, has much more to do to achieve better results in securing its cyberspace. The flaws observed in these study countries are not only technical or organizational; it is necessary to be able to resolve certain legal problems at the outset.

I.2. Legal flaws and/or inadequacies

In a report published on November 23, 2018, the CNIL presents the state of play six months after the application of the GDPR. It estimates that 66% of French people (according to an IFOP survey)[23]say they are more sensitive than before to data protection[24]and the Commission is receiving more and more complaints[25]While it is true that the GDPR offers important guarantees, there are certain aspects that escape it and are likely to create areas for violations of user rights. Indeed, France does not have a law relating to the ownership of personal data. The text of the GDPR allows the collection of various data as long as they are useful for a system. However, in accordance with Article 8, certain categories of data are excluded, including those that reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, as well as trade union membership. Similarly, it is prohibited[26] to process genetic data, biometric data intended to uniquely identify a person, health data, as well as information about the sex life or sexual orientation of a natural person.

In Cameroon, generally speaking, the legal framework for cybersecurity and the protection of personal data online (2010 laws on cybersecurity and cybercrime and the recent 2024 law on the protection of personal data) remains limited in responding to current digital challenges (lack of technological

---

[17]*Id.*
[18]ANSSI, "Overview of the cyber threat", 2024 Report, p.12.
[19]This can be due to misconfigured VPNs, weak password levels etc.
[20]CESIN, "Annual Barometer of Business Cybersecurity", OpinionWay Survey for CESIN conducted online from December 2024 to January 2025 among CESIN members".
[21]According to the National ICT Agency (ANTIC), losses linked to cyberattacks amounted to 12.2 billion FCFA recorded in 2021.twice as many as in 2019.
[22] In 2023, this method was among the most used by fraudsters since it affected 37% of French companies at least once (https://trustpair.com/fr/blog/fovi-une-technique-de-fraud-tres-plbiscitee-par-les-cybercriminels/(accessed May 12, 2025).
[23]IFOP, "French Views on the Protection of Personal Data", for Renaissance Numérique, April 2018, see the address: https://www.ifop.com/wp-content/uploads/2018/05/francais-rgpd.pdf
[24] https://www.cnil.fr/fr/rgpd-quel-bilan-6-mois-apres-son-entree-en-application(accessed May 12, 2025)
[25]Id.
[26]*Ibid*., p.37.

updates, non-categorization of offenses and data, etc.). Indeed, its legislative framework has several gaps that hinder an effective fight against cyberattacks.

Furthermore, the judicial delays linked to the organization of the Cameroonian judicial system do not make things easier.[27]. In addition, justice actors are not always sufficiently equipped to handle cases related to cyber-attacks[28] especially if they are technical. This is a set of shortcomings that the legislative framework will have to take into account and encourage. These observations mean that the countries under study will have to quickly align themselves with the legal requirements imposed by the perpetual evolution of digital technologies in order not to leave significant room for maneuver to cyber criminals. Furthermore, another major issue raised by the digitalization of society is that of the management and processing of massive data captured, stored or processed online in an illegal approach, this is the major problem of regular attacks on personal data collected online.

2. Significant and ongoing breaches of personal data online

The misuse of personal data online is rife in both France and Cameroon and undoubtedly constitutes an invasion of privacy. These violations are manifested concretely by the improper use of data collected online but also by the lack of consent of cyber users.

2.1. Improper use of data recorded online

In France, as we have seen, the GDPR prescribes explicit consent[29]which means that the data must not be used without the informed consent of the persons concerned[30]. The GDPR also limits the purpose of the possible processing of personal data collected online to the sole declared objective[31]. In addition, the GDPR enshrines the right to be forgotten[32] and data portability[33]. The sanctions regime goes up to 4% of turnover, or 20 million euros[34]. These measures applicable in France are in theory sufficient to deter, but the observation remains that the violations are significant and therefore call into question the effectiveness of the repressive regime[35]. On the other hand, in Cameroon, the penalties for violations

---

[27]See interview with NKOULOU, Commander of the Yaoundé III Research Brigade, assistant to the Public Prosecutor: "When we receive cases of cybercrime […] the absence of specialized teams leads to the files being referred to the Central Administration."

[28]See interview with Willy HAPPY, Commander of the Bafoussam 1 Research Brigade, Judicial Police Officer: "For complaints relating to cybercrime, we are very often confronted with the lack of necessary technical skills […].

[29]Under the ePrivacy Directive, Internet users must be informed and give their consent prior to the storage and reading of certain trackers. Article 5(3) of Directive 2002/58/EC, as amended in 2009, establishes the principle:

- prior consent from the user before storing information on his terminal or accessing information already stored on it;
- unless these actions are strictly necessary for the provision of an online communication service expressly requested by the user or have the exclusive purpose of enabling or facilitating communication by electronic means.

Article 82 of the Data Protection Act transposes these provisions into French law.

The CNIL points out that the consent provided for by these provisions refers to the definition and conditions provided for in Articles 4(11) and 7 of the GDPR. It must therefore be free, specific, informed, unequivocal and the user must be able to withdraw it, at any time, with the same simplicity as he or she granted it.

In order to recall and explain the law applicable to the deposit and reading of tracers in the user's terminal, the CNIL adopted on September 17, 2020guidelines, completed by arecommendationaimed in particular at proposing examples of practical methods for obtaining consent.

[30]See article 7 of the 2016 GDPR, taken up by the 2018 law in France on the protection of personal data.

[31]*Ibid*., Article 5.

[32]*Ibid*., Article 17.

[33]*Ibid*., Article 20.

[34]*Ibid.*, Article 83.

[35] Over the period 2022-2024, the CNIL adopted 495 formal notices and150 sanctions, for a cumulative fine of more than 245 million euros, including 55 million for the year 2024 alone(https://www.vie-publique.fr/en-bref/298380-protection-des-donnees-personnelles-le-bilan-2024-de-la-cnil#:~:text=Sur%20la%20p%C3%A9riode%202022%2D2024,pour%20la%20seule%20ann%C3%A9e%202024).

See also, Activity Report of the European Data Protection Supervisor of 23 April 2025

relating to the processing of personal data are significant. They fall into three categories: administrative sanctions[36], civilians[37]and criminal[38].

Thus, in France as in Cameroon, despite existing legislative measures, online data remains a prime target for unacknowledged, non-compliant uses, particularly for commercial or advertising purposes. The commercialization of personal data has become commonplace in the digital economy. Many service providers (social networks, data brokers, advertisers) collect, analyze, and resell this information, often without users' clear consent[39].These data manipulations have undeniable repercussions on privacy (identity theft, intrusive advertising), violating protection laws. In short, the sale of personal data represents a considerable reality, often unclear and abusive. Even if regulations in France and Cameroon regulate these practices, user vigilance and a more rigorous legal framework remain essential, especially in a context where violations related to consent are still very present.

2.2. Consent-related violations

In France, despite the mandatory requirement for prior user consent, consent-related violations persist and can even manifest themselves through implied consent and the failure to respect user rights. In recent years, technology giants and public institutions have been called into question and sanctioned for the abusive collection, illegal processing, or poor protection of personal data in France[40]. We can deplore the sometimes-flexible sanction regime of the CNIL, which ranges from a public warning to insignificant fines in relation to the intention.

In Cameroon, while it is true that effective sanctions are not currently being imposed on this issue, the fact remains that situations of violation of the consent requirement are legion. The operator MTN Cameroon has repeatedly been accused by users of selling their data[41]; which would allow cyber criminals to phish them. It is also a truism to note that Facebook openly violates the obligation to delete data beyond the legal period of 10 years[42]. Clearly, in both France and Cameroon, compliance with consent for the processing of personal data poses significant challenges. While in France, the regulatory framework seems better adapted to the problem, violations related to consent remain. However, the situation in Cameroon is alarming; awareness and enforcement of the legislation are derisory[43]. There is therefore an urgent need to rethink the operational framework for securing and protecting personal data online, taking into account current challenges.

II. Framework for Action in Response to Security and Personal Data Protection Challenges Online: A Global and Context-Specific Approach for France and Cameroon

To address the growing vulnerability of internet users in both France and Cameroon, it is essential to design and implement multidimensional strategies. These strategies must integrate legal, political, economic, technological, and sociocultural levers to ensure a sustainable digital ecosystem.

---

[36]See articles 54-61 of the December 2024 law relating to the protection of personal data in Cameroon.
[37]See Articles 63-70 of the aforementioned law.
[38]Article 62 of the 2024 law on the protection of personal data in Cameroon provides that in the event of serious expectations, the victim may refer the matter to the competent court in order to safeguard his or her rights and, where appropriate, depending on the seriousness of the violation, in an emergency procedure.
[39] Barraud DE LAGERIE /Emmanuel KESSOUS, The marketing of personal data or the difficult extension of the market to the individual in: STEINER, PHILIPPE, and Marie TRESPEUCH, Contested Markets, Presses universitaires du Midi, 2014, pp. 219-250.
[40] In total, the CNIL issued 331 corrective measures in 2024, including 87 sanctions for a total amount of more than 55 million euros in fines.which clearly illustrates the constant dynamics of attacks on personal data in France.
[41]
https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/t%C3%A9l%C3%A9phonie-mobile-pourquoi-les-camerounais-boycottent-orange-et-mtn/#:~:text=En%20toutre%2C%20les%20associations%20de,la%20loi%20en%20vigueur... (accessed May 30, 2025).
[42]See for example the memory recalls over more than ten years etc.
[43]See interview with MFOMKPA ABADA, judge and investigating magistrate, "most of the time, we resort to traditional legislation to deal with cases relating to cybercrime."

1. Implementation and Strengthening of Legal Frameworks for Personal Data Protection in France and Cameroon

In response to the exponential growth of digital footprints left by internet users, it is crucial to establish robust and contextually adapted legal frameworks to ensure the security and protection of personal data. This imperative varies according to the socio-political and technological contexts of the Global North (France) and Global South (Cameroon), while resting on shared principles such as transparency, accountability, and digital sovereignty.

In France, the legal framework is primarily based on the General Data Protection Regulation (GDPR), considered one of the strictest standards worldwide. It requires organizations to uphold strong principles of data protection, notably transparency and information security. A key aspect involves continuously strengthening the GDPR to adapt to technological developments (e.g., artificial intelligence) and new data processing methods via the Internet of Things (IoT) or biometric systems. As Fuster (2014) emphasizes, regulations must evolve in parallel with technological innovations to safeguard fundamental rights in a constantly changing digital environment. Moreover, the CNIL (National Commission on Informatics and Liberty) must intensify its oversight, particularly in light of emerging vulnerabilities such as ransomware attacks, phishing, and data leaks. The implementation of ethical charters for companies handling sensitive data, along with reinforced obligations for user transparency and consent, also remain priority areas. Enforcing deterrent sanctions could improve compliance with these rules.

In Cameroon, where the legal framework is still developing, the challenge lies in drafting specific laws that effectively protect data while accounting for local realities. According to Youmssi Eya (2019), the development of data protection legislation in Francophone Africa could draw inspiration from the GDPR while integrating regional socio-economic particularities. This requires a gradual implementation, tailored to technological infrastructure and cultural diversity. Law No. 2024/017 on data protection represents a significant step forward for the country, but it must be accompanied by implementing decrees that clarify its practical application and penalties for non-compliance. Harmonization with existing texts is essential to avoid inconsistencies. The establishment of a supervisory body for data protection and privacy, ensuring compliance among businesses and institutions, could fulfill this role—drawing inspiration from France's CNIL model. Finally, the legislation should include substantial fines and impose strict transparency obligations in data processing, to encourage companies to adopt a proactive approach. Indeed, deterrent sanctions help ensure compliance with data management obligations (Zuboff, 2019).

2. North–South International Cooperation for an Effective Global Response to Cyber Threats

In light of the growing global scale of cyber threats, it is essential that countries from both the Global North and South actively collaborate to establish robust frameworks for data security and protection. Such an approach relies not only on information sharing but also on the development of joint strategies to avoid fragmented responses and ensure fair and equitable data protection worldwide.

2.1. Strengthening North–South Cooperation Against Cyber Threats

Enhanced international cooperation is a key step toward improving digital security. Initiatives such as the Budapest Convention on Cybercrime can serve as a model for Southern countries, provided they are adapted to local realities to better combat online criminality. In Africa, programs like AFRIPOL already facilitate information exchange and the harmonization of national laws with international standards. Bamberger and Mulligan (2015) emphasize that data protection should be recognized as a fundamental right, which could foster a spirit of digital solidarity regardless of economic or technological disparities. Cooperation with international organizations is also crucial for standard harmonization and information sharing, through collaborative platforms or partnerships with

institutions such as the World Bank, aimed at strengthening cybersecurity. This collective approach enhances resilience against escalating cyber threats.

2.2. Establishing an International Criminal Court for Cybersecurity

Another strategy involves considering the creation of an International Criminal Court dedicated to cybercrime. Such a tribunal would enable a coherent and coordinated response to transnational offenses. It could not only prosecute cybercriminals effectively but also develop a harmonized legal framework that facilitates mutual recognition of judgments and extradition procedures. However, establishing such an institution requires global political will and cooperation among states to share technical and legislative expertise, ensuring its effective operation.

2.3. Skills Transfer and Local Capacity Building

Finally, the transfer of expertise and the development of local capacities are essential to address cyber challenges. Institutional twinning programs (North–South) or bilateral partnerships (e.g., France–Cameroon) can play a vital role in sharing technical knowledge and training local experts—judges, law enforcement officers, and cybersecurity professionals—capable of anticipating, detecting, and responding to cyber threats. This would significantly strengthen the resilience of these countries. As Bamberger and Mulligan (2015) point out, best practices in personal data management contribute to a collective defense against cyber threats.

North–South cooperation must be grounded in an inclusive and collaborative approach. By combining these various levers—international cooperation, the creation of a specialized tribunal, and the development of local expertise—the global community can build a coherent, fair, and effective response to contemporary digital challenges. Harmonizing efforts is essential to reinforce the security of digital exchanges and facilitate international cooperation (Osula et Rõigas, 2016).

3. Strengthening the Responsibility of Organizations and Individuals through Education, Awareness, and Good Online Practices

It is essential to reinforce the responsibility of public and private actors in managing personal data online in order to better address the security challenges linked to users' digital presence. This approach relies on several pillars, including education, awareness, the implementation of strict policies, the adoption of advanced technologies, and compliance with international standards. These measures aim to promote accountability among these stakeholders.

First and foremost, training and awareness play a central role. In France, despite a robust legislative framework such as the GDPR, education remains a key lever for building a better-informed society. It is necessary to integrate current modules on data protection into school, university, and professional curricula. These trainings should be practical and include cyberattack simulations to demonstrate common vulnerabilities. It is also crucial to offer up-to-date training tailored to emerging threats, in collaboration with tech companies and NGOs. Furthermore, awareness programs should not only focus on the technical aspects of digital security but also on understanding the importance of data privacy. Public campaigns, such as those led by Cybermalveillance.gouv.fr, could be expanded to include localized interactive workshops targeting all age groups. The "No More Ransom" campaign, which has been successful in Europe, could inspire French initiatives by incorporating podcasts and videos on best online practices.

In Cameroon, schools—starting from the primary level—should include courses on digital rights and online security tools. As suggested by Couldry and Mejias (2019), a culture of security must be established at all levels, centered on the responsible use of digital tools. A national awareness campaign, translated into local languages, could leverage popular social media platforms such as Facebook and TikTok to maximize the impact of messages promoting good online practices. Encouraging the creation of participatory content on online safety also helps reinforce ownership of these messages. Indeed, well-informed users adopt safer behaviors, which contributes to reducing their vulnerability and that of digital systems.

Businesses also have a role to play in developing a culture of security, particularly through ongoing training of their employees on data collection, processing, and protection. Regular cybersecurity awareness among staff significantly improves vigilance and responsiveness to incidents. The implementation of clear security policies and the adoption of advanced protection technologies are indispensable. The adoption of recognized standards, such as ISO 27001, provides a reliable framework for managing digital risks (Chesbrough, 2019), by structuring information security management systems (ISMS). Technology must also be at the heart of this approach: the use of strong cryptography (notably end-to-end encryption), multi-factor authentication, and artificial intelligence (AI) for anomaly detection. These tools would help establish a defense against intrusions and data leaks. Moreover, regular system updates and prompt vulnerability remediation must also be prioritized.

Conclusion

The digital footprint of Internet users, a reflection of their digital interactions, is now a major strategic issue in global digital governance. Despite legislative efforts and other measures put in place to ensure the security of ICT use, there has been a resurgence of cyberattacks in both the Global North and the Global South, particularly between France and Cameroon. Moreover, the growing online attacks on personal data reveal worrying flaws in digital governance mechanisms. However, there are profound disparities between these two countries in terms of security and the protection of personal data. These disparities are not only technological or legal, but also stem from sociocultural, economic, and political factors.

In France, the General Data Protection Regulation (GDPR) represents an advanced legal framework, guaranteeing citizens a degree of control over their personal data (Rossi and Bigot, 2018). This regulation, praised for its extraterritorial scope and its requirement for transparency, has inspired several countries in the Global South. However, as Maciel-Hibbard (2018) points out, this transposition often remains theoretical in countries where legal and technical infrastructures are insufficient. In Cameroon, although legislative texts exist (such as Law No. 2010/012 on cybersecurity and cybercrime and the recent 2024 law on the protection of personal data), their application remains limited by a lack of resources, training, and awareness. This situation creates an environment conducive to data abuse (massive collection of personal data, often without users' knowledge, exposing them to increased risks of surveillance, manipulation and identity theft), aggravated by a weak culture of privacy where users are less informed of their rights and more vulnerable to abuse and an often-communal perception of digital identity.

Furthermore, Nissenbaum's (2009) work on the concept of "privacy as contextual integrity" reminds us that privacy cannot be understood independently of its cultural and social context. This point is crucial from a North-South perspective, where Western data protection standards do not always correspond to local realities. In this context, it becomes imperative to rethink personal data security strategies at the "glocal scale". A transdisciplinary approach, combining law, sociology, management and technology, is necessary to design solutions adapted to local specificities while respecting international standards. Three lines of action emerge from this analysis: 1- Implementation and strengthening of legal frameworks for the protection of personal data in France and Cameroon; 2- North-South international cooperation for an effective global response to cyber threats; 3- Strengthening the responsibility of organizations and individuals in the face of cybersecurity issues through education, awareness-raising and the adoption of good digital practices.

In short, this research calls for a rethinking of current digital governance paradigms. The digital footprint should not be seen solely as an economic resource, but as an extension of human identity, deserving protection and respect. France and Cameroon, as representatives of two contrasting realities, have a key role to play in building a more ethical, inclusive, and sustainable digital space. While this research sheds light on the issues related to online security and personal data protection in a North-South context, it nevertheless presents limitations that present avenues for future research. These include in-depth comparative analysis between countries in the Global South, such as

Cameroon, Senegal, or India, in terms of legislation, digital infrastructure, and perceptions of privacy, in order to better understand regional dynamics and avoid a homogenous vision of the "Global South." Furthermore, the study of sociocultural representations of privacy, through qualitative approaches such as interviews and focus groups, would make it possible to assess the impact of cultural norms on digital behaviors and the acceptance of data protection policies. It would also be relevant to explore the adaptation of emerging technologies, such as artificial intelligence, metaverses, blockchain, or homomorphic encryption, in resource-limited environments, to see if these innovations can respond to the realities of countries in the Global South. Finally, another axis concerns the mapping of digital vulnerabilities of marginalized groups, particularly women, youth, or rural populations, through field surveys and intersectional analysis to identify specific risks of cyberviolence or data exploitation.

Bibliographic References

- **Bamberger, K. A., et Mulligan, D. K. (2015).** *Privacy on the ground: driving corporate behavior in the United States and Europe*. MIT Press.
- **Chesbrough, H. (2019).** *Open innovation results: Going beyond the hype and getting down to business*. Oxford University Press.
- **Clarke, R. (2014).** The Nature of the Digital Persona and Its Implications for Data Protection Law.
- **Clarke, R. (2019).** Risks inherent in the digital surveillance economy: A research agenda. *Journal of information technology*, *34*(1), 59-80.
- **Commission Européenne (2018).** Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données – RGPD) – Corrigendum. Journal officiel de l'Union européenne, L 127, 23 mai 2018, p. 2-13. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
- **Couldry, N., et Mejias, U. A. (2019).** *The Costs of Connection: How Data Are Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
- **Digital Report (2025).** Digital 2025: Global Overview Report – Essential insights into Internet, social media, mobile and e-commerce use around the world. Londres : We Are Social / Meltwater. Publié le 5 février 2025. Disponible en ligne : https://wearesocial.com/digital-2025 (consulté le 29 mai 2025).
- **Fuster, G. G. (2014).** *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business.
- **Interpol (2022).** Cybercrime in Africa: Challenges and Opportunities. Lyon : INTERPOL, Cybercrime Directorate / African Cybercrime Operations Desk, octobre 2022. 68 p. ISBN 978-92-95055-59-1. Consultable en ligne : https://www.interpol.int/en/content/download/18634/file/Interpol_Cybercrime-in-Africa_2022.pdf
- **Maciel-Hibbard, M. (2018).** Protection des données personnelles et cyber(in)sécurité. *Politique étrangère,* Été (2), 55-66. https://doi.org/10.3917/pe.182.0055.
- **Milan, S., et Treré, E. (2020).** *Latin American Visions for a Digital New Deal: Towards Buen Vivir with Data*. https://projects.itforchange.net/digital-new-deal/2021/01/25/latin-american-visions-digital-new-deal-towards-buen-vivir-data/ .
- **Nissenbaum, H. (2009).** *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.
- **Osula, A. M., et Rõigas, H. (2016).** *International cyber norms: Legal, policy & industry perspectives*. NATO Cooperative Cyber Defence Centre of Excellence.
- **Rossi, J. et Bigot, J.-É. (2018).** Traces numériques et recherche scientifique au prisme du droit des données personnelles. *Les Enjeux de l'information et de la communication*, 19/2(2), 161-177. https://doi.org/10.3917/enic.025.0161.
- **Solove, D. J. (2006).** *A Taxonomy of Privacy*. University of Pennsylvania Law Review, 154(3), 477–560. https://ssrn.com/abstract=667622
- **Statista Research Department (2024).** « Nombre d'utilisateurs Internet et des réseaux sociaux dans le monde en janvier 2024 (en milliards) ». Statista, publié le 12 septembre 2024. Disponible en ligne :

https://fr.statista.com/statistiques/1350675/nombre-utilisateurs-internet-reseaux-sociaux-monde/ (consulté le 29 mai 2025).

- **Union internationale des télécommunications – UIT (2020).** *Manual for Measuring ICT Access and Use by Households and Individuals – 2020 Edition*. Genève : UIT, Bureau du développement des télécommunications. ISBN : 978-92-61-30861-2 (version PDF). Disponible en ligne : https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-ITCMEAS-2020-PDF-E.pdf
- **Union internationale des télécommunications – UIT (2023).** « Mesurer le développement numérique : Faits et chiffres 2023 » (Measuring Digital Development: Facts and Figures 2023). Genève : UIT. ISBN 978-92-61-37031-4. Disponible en ligne : https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (consulté le 29 mai 2025).
- **Walczak, N. (2014).** *La protection des données personnelles sur l'internet. Analyse des discours et des enjeux sociopolitiques*. Doctoral dissertation, Université Lumière Lyon 2, France.
- **Youmssi Eya, Y. L. (2019).** *La protection des données informatiques à caractère personnel au Cameroun*. Mémoire de Master Droits de l'Homme et Action Humanitaire, Université Catholique d'Afrique Centrale. Disponible sur Academia.edu : https://www.academia.edu/42136727
- **Zuboff, S. (2019).** The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. *Social Forces*, *98*(2), 1–4. https://www.jstor.org/stable/26862460