United Nations A/HRC/43/NGO/58

General Assembly

Distr.: General
12 February 2020

English only

Human Rights Council
Forty-third session
24 February–20 March 2020
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Human Rights Advocates Inc., a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[01 February 2020]

* Issued as received, in the language(s) of submission only.

GE.20-02090(E)
2002090

The Right to privacy in the Digital Age

Introduction

Human Rights Advocates applauds the Human Rights Council in addressing the emerging issues on individuals' digital privacy rights. Certainly, significant strides have been achieved in protecting individuals' information from being sold, shared, improperly used, or accessed without their consent or knowledge. Human Rights Advocates celebrates and acknowledges the work done by the Human Rights Council and the Special Rapporteur on Privacy Rights, in the effort to promote and ensure the protection of personal digital data in an era where access to private personal information is a click away. Defending privacy rights is crucial as it has a direct effect on personal autonomy.

However, because there is no consensus on the protections that should be in place or what type of information should be protected, personal information is at risk of being distributed or accessed without owner's consent since non-state and state actors are improperly sharing, storing, and profiting from collected individuals' information. Human Right Advocates urges the Human Rights Council to call upon States to adopt a universal standard for the protection of people's digital private personal information. One of the major problems with ensuring an adequate level of data protection is due to the very nature of digital information — it can be accessed from anywhere. Therefore, even where regions have comprehensive data protection regulations, States have little power over non-state actors that operate outside of the jurisdiction. For instance in the European Union (EU), which has legislated to ensure substantial protections for their citizens, individuals' data is still at risk. Even when the legislation requires outside non-state actors to comply with the regulation there is a question as to the extraterritoriality and its enforceability. Hence, it is crucial that all States adopt measures with the same standard of care and diligence ensuring people's personal data is protected.

Digital privacy Rights

The right to privacy is a fundamental right that has long been recognised by governments around the world. The first time the international community stated the right to privacy was in the Universal Declaration of Human Rights Article 12 where it is articulated as "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Before the growth of the digital era, privacy rights concerned mostly the person, access to their dwelling, and access to correspondence. However, privacy rights encompass also the personal information that can be accessed and stored online. As pointed out in the Special Rapporteur 2019 Report on Privacy Rights is important to protect individuals' personal information online as it concerns a person's autonomy.

Currently the most concerted effort in addressing and evaluating cybersecurity is by the United Nations through its International Telecommunication Union, which conducts the Global Cybersecurity Index. The index's purpose is to determine the status of cybersecurity worldwide and promote global harmonization of cybersecurity legislation.

Examples of Digital privacy rights

Discussions and regulations on the right to privacy need to be addressed at a domestic and international level to be effective otherwise the gaps in protection still leave data at risk. Lack of such protections could lead to undue influence on individuals' human rights.[1] Following

[1] Human Rights Council Res. 42/15, The Right to Privacy in the Digital Age. U.N. Doc. A/HRC/RES/42/15 (Sep. 26, 2019)

are examples of legislation on data protection, cyber security, and surveillance and the effects.

EU General Data Protection Regulation (GDPR)

The GDPR is perceived as a groundbreaking legislation that addresses many of the concerns of data protection. The legislation addresses not only data protection but also cyber security; it has also provided a standard of care and regulation for all the EU and guidelines on how to enforce the legislation. The legislation establishes that controller and processor of personal data must put in place "appropriate technical and organizational measures to implement the data protection principles."[2] GDPR is consumer first focused, therefore it is aimed at protecting individuals' information. Further, it encompasses entities that although operate outside Europe or the European Economic area, they must adhere to GDPR guidelines and requirements if they deal with people in Europe.

Paris call for trust and security in cyberspace

On November 12, 2018, French President Macron called for a worldwide effort from States and non-state actors to unite in an effort to combat, prevent and recover from malicious cyber activity that harm individuals and critical infrastructure. This type of legislation although greatly needed because it deals with cyber security and promotes personal digital privacy rights, the call does not address the problem that there is a need worldwide for legislation relating to surveillance, big data, open data, health data, protecting consumer and personal data online and how State and non-State actors are allowed to access, store, or share the obtained information.

California consumer privacy act

The state of California in the United States of America enacted a law in 2018, which entered into force on January 1, 2020 where it allows consumers to ask business to disclose the personal information the business has gathered on the individual, how it has shared such information, and gives the consumer the opportunity to opt-out from the business disclosing their information to third parties.[3] However, this the only state that has enacted this protection for their citizens so if the individuals' information is accessed in a different state, it in effect nullifies the state of California's efforts to protect its own citizens' private information. Hence, there is need a comprehensive federal privacy law in the United States[4] that would give users the right to have their personal data minimized, give users the right to know what data is collected on them, give users the right to access that data, and require that data be kept securely.

Countries with the worst privacy protection and extensive surveillance of their citizens

Comparitech, a consumer protection focused website, conducted an assessment out of 47 countries to evaluate on privacy protection and surveillance, scoring them from 1-5 (5 being the best and 1 the worst). The assessment found that the top five countries with the worst privacy protection and extensive endemic surveillance were: China, the Russian Federation, India, Thailand, and Malaysia.[5] Following is an explanation on why experts have found China to lack in digital privacy rights protections.

[2] European Union, General Data Protection Regulation, Art. 25.2, available at: https://gdpr-info.eu/art-25-gdpr/

[3] CA Civ. Code Section 1798.100, available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018

[4] United States in the Comparitech Assessment scored a 2.7 tying with Singapore because although there are some safeguards, there are weakened protections. The assessment also found that the countries with the best privacy protection are in the EU and accredits in part the GDPR to their data protection efforts.

[5] *Id.*

The Comparitech assessment found that despite China having privacy laws, the laws lack guidance and therefore difficult to enforce. Some of the concerns expressed by Comparitech were: State practices sharing personal data among agencies; there is no legislation on how long personal data can be stored, yet there are specific guidelines on what data needs to be stored by the state and non-state actors; and data recollected for medical reasons are often misused under the guise of "public interest records."[6] While the lack of data protection is used for state surveillance it has also contributed for the easily accessible data to be misused by individuals for private extortion and fraud.[7]

It is important to note that late 2018, China announced it has placed personal data protection legislation on the agenda and on June 2019 the government released a set of guidelines to be followed by different mobile apps.[8] The guidelines were regarding informed user consent and what information can be accessed by the mobile apps. Although it does not solve the privacy issue, it a start towards comprehensive legislation. Concern has been expressed on whether the government will enforce this temporary regulation.[9]

Conclusion

Digital data privacy is a prevalent issue today. Data privacy encompasses many aspects such as: security and surveillance; big data and open data; health data, and the use of personal data by state and non-state actors. In the absence of clear legislation and effective enforcement, individuals' information is at risk of being improperly used, collected, and access which could lead to extortion, fraud, and overreaching surveillance.

HRA recommends that the Human Rights Council:

- Ask States to make data protection and cybersecurity a priority;
- Ask States to create comprehensive domestic legislation to protect privacy rights online; and
- Call for a universal global legislation on data protection and cybersecurity.

---

[6] *Id.*

[7] Feng, Emily, "In China, A New Call To Protect Data Privacy," NPR, (January 5, 2020), available at: https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy

[8] Ma Wenyan, Wiston, "China is waking up to data protection and privacy. Here's why that matters," World Economic Forum, (November 12, 2019), available at: https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/

[9] *Id.*