INTERNATIONAL JOURNAL FOR INNOVATION EDUCATION AND RESEARCH
ISSN: 2411-2933

Journal URL: https://scholarsjournal.net/index.php/ijier

DOI: https://doi.org/10.31686/ijier.vol13.iss4.4279

The Right of Privacy in the Digital Age

Jinan Al Toufaily[1]

[1]*Assosciate Professor/Islamic University of Lebanon*

Abstract

Living in modern society, we are profiled. We accept the necessity to hand over intimate details about ourselves to proper authorities and presume they will keep this information secure-only to be used under the most egregious cases with legal justifications. Parents provide governments with information about their children to obtain necessary services, such as health care. We reciprocate the forfeiture of our intimate details by accepting the fine print on every form we sign-or button we press. In doing so, we enable secondhand trading of our personal information, exponentially increasing the likelihood that our data will be utilized for illegitimate purposes. Often without our awareness or consent, detection devices track our movements, our preferences, and any information they are capable of mining from our digital existence. This data is used to manipulate us, rob from us, and engage in prejudice against us-at times legally. We are stalked by algorithms that profile all of us. This is not a dystopian outlook on the future or paranoia. This is present day reality, whereby we live in a data-driven society with ubiquitous corruption that enables a small number of individuals to transgress a destitute mass of phone and internet media users.

Key words: Children privacy, digital age, parents, ICCPR

INTRODUCTION

People always feel profiled in this modern society, as they acknowledge the need to give up insights about themselves to authorities, assuming to keep secured data that would only be utilized in the most intolerable cases with legitimizations (legal justification). Health care or medical care is an example of what parents provide to governments about their children in order to give sufficient data about their children to get or obtain the essential services (Wlado,2007). Tolerating the fine print on every button people press is how they relinquish the forfeiture of intimate details. Hence, this way empowers the second-hand trading of the personal data which lead to an increase in using this data for illegitimate reasons (Wlado,2007).

Only by the digital existence of individuals, can lead to empowering the capability of mining any data (Snowden,2013). Also, frequently without the people's consent or mindfulness, whether they like it or not, there is always detection devices that track their preferences, locations and any movements (Snowden,2013). However, this information mining is to control, rob and manipulate people, where it could engage them in prejudice that is against them legally (Wlado,2007). In this digital age, human beings are always being followed and stalked by a huge number of hackers, which is definitely not a tragic attitude toward the future or paranoia. For the past few decades, we have been living in a data-driven society and the ugly reality is that there is a pervasive corruption that is empowering some individuals to violate a penniless mass of phone and

social media users (Wlado,2007). On the other hand, with the appearance of digital privacy, people are freer on the internet since they are more secured. So, individuals have the right to freely exist on the internet, where they also have the right to not being interrupted by any data by choosing the data they want to exist or be exposed to them on the internet (Wlado,2007).

Nowadays, the present society and the contemporary life could be called “The Transparent Society” where communication technologies like smartphones and unlimited free internet plays a huge part of this society (Polonetsky,2017). In addition to the spread of information through a digital form. Entertainment, medical, educational and social services are all found and provided online. On the other hand, the border between the individual, state and private enterprise is being dissolved by the data technologies and computer systems that are capable of recoding every individual’s keystroke and actual development (Wlado,2007). Therefore, this present society is the “Digital Age”.

Moreover, The Committee on Privacy in the Information Age depicts these advances as "better approaches for gathering and dealing with data that thus have repercussions all through society, as they intercede a lot of private and public correspondence, association, and exchanges" (Waldo,2007).

According to Bernal, there is still a lack of transparency, not only the search engines functions but also the governments internet surveillance where the information is considered saved after it was erased (Wlado,2007). Civil society may be acquainted with online data savings of locations, IP addresses and communication, but still think that there is nothing to be worried about or hide. This rapid development in information technology is turning into a disputable subject of much discussion as well as threatening human rights on several levels (Polonetsky,2017). The United Nations High Commissioner for Human Rights (UNHCR) diagrams the manners in which digital communication technology has improved and developed enjoyment of human rights, boosted the freedom of expression, worked with worldwide discussion and cultivated democratic cooperation (Polonetsky,2017). While others argue that these digital information technologies improve the realization of human rights and freedom.

The best tool in order to protect human rights, is the surveillance of electronic communications data which is considered to be very beneficial and effective for legal needs or enforcements (Polonetsky,2017). Hence, this was reflected and deducted from a debate about terrorism and security when conducted in consistence with the law. In contrast, interception, assortment of personal data and facilitating or working with surveillance, is now considered a huge threat on basic freedoms. Globally, the invasive digital surveillance has made some places a perpetrator and a victim, for instance: the private sector, the public sector, the entities of government (Wlado,2007).

The technological platforms whereupon worldwide political, monetary and public activity are progressively dependent are not just helpless against surveillance mass observation, they may really work with it" (Wlado,2007). The presentation of the powerful and amazing individual computation technology to the consumer market have brought the similar strategies of impedance and control to the singular level, reclassifying the contemporary wilderness of basic freedoms, with the presence of the surveillance and reconnaissance that have been a part of the sociopolitical reality (Snowden,2013).

Enumerating mass surveillance by US National Security Agency, the right to privacy and its insurance is by

all accounts truly jeopardized and made new degrees of discussion (Snowden,2013). In addition, in today's Information age, the most aspects discussed and worried about is the subject of privacy (Waldo,2007).

Therefore, individuals protecting and being mindful about their computers, mobiles, tablets and other devices connected to the internet, is known as "Digital security". These could be in the form of hacking (Polonetsky,2017). Adding to that, one could protect their personal data from being used and sold by companies by using digital security, so there are numerous ways to protect data online, for instance: VPNs, password managers and identity monitoring services (Snowden,2013).

Privacy

Data privacy alludes to how to oversee information dependent on its apparent importance. Privacy was a critical element of human existence. Be that as it may, more significance is appended to data privacy as long as the more data is digitized and more information is communicated online. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. Moreover, privacy is now considered as a human right, where it is recognized in many international and regional treaties, for instance, UN Declaration of Human Rights, the international covenant on civil and political rights (ICCPR,1966). Privacy is significant in light of the fact that: Privacy enables individuals to pick their contemplations and sentiments and who they share them with. Thus, privacy ensures people's data that don't need shared openly (like wellbeing or individual accounting records), as well as, it ensures their actual wellbeing (if the continuous area information is private). Bad things can happen, if privacy got into the wrong hands. Once the data gets in the wrong hands then privacy should be kept private. A data breach at a government agency can put proprietary data in the hands of a competitor or put top secret information in the hands of an enemy state. California passed a groundbreaking new digital privacy protection law during the year of 2018. In addition, companies in California gave the permission to consumers to ask them not to sell their personal information. The law expressly shields them from retaliation if won't permit its sale.

Thus, when the government has easy access to this information people loose more than just privacy and control over their information. Technological innovation has outpaced the privacy protections. As a result, the digital footprint can be tracked by the government and corporations in ways that were once unthinkable. As much as it gets difficult to prevent data leakage scandals, the governments and companies are still trying to make positive impact and changes to protect online privacy. Thus, Privacy is not dead in an online world, but it might be a long way for personal paid model to become reality.

The concept of privacy in the digital age

Protection is about decision, the decision to uncover or not to uncover, insights concerning themselves in their life. Individuals, who drew the complex and flawless pictures of creatures in caverns like those in Lascaux in France, did as such in profound and dim environmental elements. Their craft was intended for the chose not many and they regularly "marked " their works of art by blowing color over their hand to make some meaningful difference, a sort of early biometric. People have consistently perceived the idea of protection and utilized it to uncover. These early individuals decided to uncover a piece of what their identity was and this ethos of what protection is, stays with us today.

At the point when we enter our work environment, we may "clock in" showing what time we showed up. At

the point when we hand over our bank card to the bistro at noon to purchase our lunch, the bank currently realizes that we were at that shop and burned through $10 at 12 early afternoons on Tuesday. Returning we settle on a decision to our accomplice to tell them our appearance time, the telephone organization then, at that point, knows our area and which number was called.

As people head into a period where they are characteristically associated, to their devices and gadgets and each other through the Internet of Things, protection will turn into a considerably more different and complex scene. We really want to go ahead into this new period with a more profound comprehension of how to ensure protection privileges are kept up with and regarded.

Therefore, privacy as an idea has not changed in a long time since Homo sapiens appeared, however protection as an activity has changed, and the advanced age has acquainted layers of intricacy with the fundamental idea of protection that we want, as computerized residents, to disentangle and comprehend.

Digital age

What spread out the initial move towards giving the capacity to move and transfer data openly and rapidly, is the presentation of the PC with ensuing innovation introduced. In the time period starting in the 1970s, this has been characterized as the Information age.

I. Violations of Privacy

A. Search and Seizure of Digital Property

In order to shape the public's beliefs and curb dissent, the government and assailant organizations use Internet censorship. However, there is harassment of bloggers activists and political opponents in all countries whether developed or the least developed, where they are also being silenced. The personal data of individuals is saved, this data is utilized to profile people who seem defiant. The analysis in the name of internet privacy and security depends on the characteristics that foresees hazardous practices and behaviors being done. On the other hand, the governments were able to extract data from mobile users during some major protest movements around the world such as, the Arab Spring, the Umbrella Movement and the occupy protests. The dissuasion of protestors was done by the routine of blocking and tracking social media and other internet-based correspondence. Some laws that exist in most countries to protect search and seizure of physical property do not abide for digital property. However, it becomes passable to demand that people relinquish admittance to online media records without a court order, thus, to acquire services like visa or visit another country. Oppressive systems investigate explicit people as a technique for segregation.

B. Profiling of Marginalized Groups

In this modern age, Specific ethnic, gender and age groups are being targeted by the police. For example, the prediction culprits and victims of gun violence is done by the implement of a "Strategic Subject List" in Chicago by the Chicago police. There is a hazardous potential of a large data, mining due to the presence of the online profiling that enables the police to invade digital property of strategic subjects. The characteristic of these individuals is what the police depend on in order for them to be intimidated or arrested. However, the

disproportionate incarceration of marginalized groups is broadened due the policing practices that are being used. Another example is, the "Police Cloud" which began in China. The "Police Cloud" is responsible for tracking social and ethnic groups and it shows that they are very capable in performing these practices. Adding to that, the legal and illegal organizations have to do with profiling marginalized groups which means it's not only the police's job. Hindered groups are obvious objectives of monetary or financial scams and they are more threatened to be taken advantage of. This can be reflected by luring women into prostitution rings or refugees into forced labor.

C. Biometric Dangers

Biometric data opens an entryway for data to be hacked and mishandled although it is a unified order that professes to have a full oversight and complete control. Today's society is generally driven by computers and technology that preserves biometric data. Thus, this creates an overall worry about the destiny of this free world. People who lack technological and financial means to protect their privacy are the ones who are mostly to be penalized with vast for minor infractions as long as this data develops. However, what is never forgotten the discrimination of Nazi Germany that taught us about the danger of collecting registries that track minorities for countries. For instance, In the year of 2017, in Brazil, the Brazilian Federal Police made an arrangement with electoral court for sharing this data set without reporting the practice beforehand. However, it was presently compulsory to be included in the biometrical database which additionally empowers voting in elections.

D. Censorship

Nowadays, it is easier for governments to eliminate or erase content from the internet, while it was difficult for autocracies to track down and burn books. Some countries have a huge censorship to the point that it has self-censorship, for instance, China, Turkey and many other nations. Thus, this censorship exists in most countries where people are willing to express themselves online and are exposed to reciprocity. One of the countries that a bill was introduced to recently that provides the court with automatic access to remove content from platforms is the Zionist entity. Such activities are defended as a guard against clashes with associations. Notwithstanding, the Zionist entity Democracy Institute (IDI) contended illegal and argued against the law, as it is obligated to make create censorship in an ill-advised legitimate cycle that has no point of reference in different nations. Companies censor content but governments want to restrict online media. Thus, the inside rules of such censoring also merit oversight.

E. Business Surveillance

Facebook is an online platform that empowers and enables individual to impart private information about themselves to others who they know and trust. The Facebook Company has over than 2 billion users. Also, Facebook works well in protecting its user's data. Some detailed data like contacts, phone numbers were being gathered and shared without the individual's assent or mindfulness, through the unclear consent of sharing data with a third-party application.

Facebook has also given administrative staff control over how posts are deleted, but users do not have the same level of control over their own information. Organizations like Equifax, which collect the credit ratings of millions of people, are hacking the system. Insurance companies acquire large amounts of data from medical institutions to create predictive formulas to determine risk pools and determine percentages. More and more companies are using big data to analyze their customers. Thus, Facebook isn't the only company accused of violating user privacy. The United States, once at the forefront of privacy restrictions, passed legislation in 2017 abolishing the tradition of net neutrality. The restriction of freedom of expression and the empowerment of big data companies to massively monitor and sell information about consumer content, purchases and other personal data is all the result of this decision of abolishing the tradition of net neutrality. Google and other enormous web search destinations as of now take part in such practices. They offer our data to promoters, back up plans, and campaigning gatherings, making the world that people are presented to with practically no outside moral oversight.

Efforts to Protect Privacy

a. Multinational Efforts to Protect Privacy

Despite negative trends in the digital age, the right to privacy is still championed as an ideal by most of us. Multinational collaboration to protect digital rights is on the rise. Nations are bonding together to establish privacy-by-design controls that will protect data according to commonly agreed fundamentals. Governments, businesses, and criminal organizations have profited by invading people's privacy, and supranational bodies are a potential buffer- a last line of resistance. The European Union recently adopted the General Data Protection Regulation (GDPR,2018). The regulation demands that individuals retain control of their data, that they can see the information about them that is being collected and ask to remove this information from internet platforms. Organizations that collect data must employ a data protection officer, who will oversee that privacy standards are upheld and personal data of those who request to be forgotten are removed. A sort of multinational agencies purpose to guard our virtual rights, along with the organization that we represent, Pirate Parties International. Multinational tasks are made feasible with the aid of using member states who participate. The International Conference for Data Protection and Privacy Commissioners (CDPPC, 2020), for example, has been bringing collectively authorities stakeholders to help them satisfy their mandates. Each member country sends records safety officials to collaborate, which furthers our purpose of harmonizing facts safety. The UN Resolution at the Right to Privacy in The Digital Age additionally exemplifies a nice multinational attempt to shield privacy (UN, 2019).

b. Government Efforts to Protect Privacy

Governments can make certain that residents are made privy to personal data this is accumulated approximately them, in addition to showing facts approximately what it does with that information and its personal work. Medical facts, for example, people will be discriminated towards for employment and insurance if these medical personal statistics that governments frequently enact rules to guard is not found. A critical query that has been posed at the proper to privateness is whether or not to offer human beings with get admission to clinical statistics that display genetic tendencies to disease, as these facts might not offer

superb help whilst preventative precautions do now no longer exist. Moreover, Governments should debate the tiers of privateness and transparency which might be with inside the great hobbies of its residents. What assures the loose preference underlying the spirit of elections is the voter rights to privacy which are critical in democratic nations. Cyber security is likewise a countrywide duty as worldwide conflicts among realms frequently spill over into virtual environments. Recent examples of presidency rules to offer more transparency of privateness practices, consist of the Canadian Parliament's Privacy Commissioner's Guidelines for Online Consent and Brazil's "Internet Bill of Rights". Such rules frequently seek to adjust person consent and set up oversight into the interactions of people with net vendors and platforms. Therefore, while governments are demonized as infiltrators of our privateness, they're additionally guarantors of our virtual rights and may reprimand folks who violate them. Legislation that safeguards touchy information is vital, and many nations are suffering to maintain tempo with improvements in records era which have improved the area of virtual rights. Governments should each guard privateness and sell transparency, obligations which can appear at odds with each other however frequently feature in tandem.

c. Business Efforts to Protect Privacy

Effective on-line organizations recognize the significance of consumer trust, and that they frequently offer their customers with records safety and transparency approximately how they acquire and use facts. Single-sign up frameworks gift a venture and possibility for protective people' privateness. Users are accused of a "privateness paradox", wherein they're inclined to surrender their rights to privateness for the sake of comfort however are although outraged to study their records become applied. By permitting customers to opt-in, corporations are mitigating a few privateness invasion, however they have to cautiously weigh the benefits and drawbacks of buying and selling purchaser information with outside offerings. Data-pushed generation is an essential phenomenon, that may help us in our lives. Standardizing the privateness regulations for single-sign-on frameworks enables to make sure that consumer information isn't always misused through secondary carrier providers. Privacy improving technology help us to defend our statistics, and such offerings are frequently supplied freed from cost. Facebook, which has already been applied as a terrible instance of violating privateness, has additionally made wonderful efforts to defend our privateness through permitting customers to delete money owed and promising to allow customers to additionally be capable of delete particular statistics with inside the future. The improvement of encryption offerings has additionally accelerated the proper to be "out of the system", offering people with a virtual platform to congregate without worry of presidency interference. Furthermore, blockchain generation is increasing the proper of people to set up monetary networks that aren't authorities regulated. Efforts with the aid of using groups to defend virtual privateness need to offer mutual advantages for people and organizations.

Impact of Digital Age on People's Lives

The internet is considered to be a background utility where it is only noticed when it's absent. However, the present generation and the coming generation will be known as the digitally native born. It will be effortless for smart homes and smart applications to encompass every part of the man's lives.

Technology will be obliging and controlling humans by letting them abide its rules and regulations. As time passes and days go by, everything is developing and speeding up and becoming more complex. It's the age where humans have the power and right to access nearly all human knowledge that exists in life with only a few clicks on the buttons of their computers and phone. Thus, as technology keeps growing, this free and unlimited access to the internet will encompasses easily and effortlessly.

For example, oil is less valuable than data in this digital age life that is truly information-driven, this could lead to some companies lashing out to know what drives customer interest. Spending money wisely in the right places and the right time which saves the company the time and money is a result of the insights gained from refining data. On the other hand, even the average person has been considering social media as a part of everyday life and this will continue. Some

Some social platforms are rising to an astounding number such as, in 2020, Facebook users are estimated to be 2.6 billion, 1 billion for Instagram users and 330 million for twitter users, all these numbers fall short behind search engines (Statista,2019). Google could reach 6.9 billion searches every day, which could make me people feel thankful and glad that they would be working from home more often, avoiding the settlement in big cities where the prices of house rental or real estate create a huge burden and a waste of money in their lives (Techjury,2018)

Relocation of homes

Relocation of homes today is the total opposite of the relocations that happened in the past when millions of people were increasing the home prices, cramping up spaces and flocking in cities. Nowadays, some people prefer to sit in their office and roam big cities, paying expensive rental that will be on decrease later on. While others seek digital nomad lifestyle where they settle down in the countryside. Thus, people are capable of working from home or remotely with just a click of button using only a laptop and the internet. However, it is still essential for people to be mindful and aware about protecting their data by using VPN, when they travel since some countries still ask for VPN in order to have the right to access social media and search engines without getting worried. Thus, a main point with all that shouldn't be forgotten which is the risk of exposing privacy and interest online

The Rise of Startup Companies

The rise of Start Up companies used to be considered as the high technology innovation that was created by the U.S ecosystems, this was in the year of 2020, where Silicon Valley, Seattle and Newyork got their reputations. These startups that started with the U.S ecosystems are actually going global now, where they could be found in Shenzen, Berlin, Stockholm and Mumbai. Thus, these startups are expanding in every direction and the countries that are using it are now becoming the startup capitols at their own pace. Moreover, what is considered a huge interruption in human daily life nowadays is all digital with the increase of startups to the extent that they are transforming into mega-corporations.

In this decade, TV is becoming from the past while online entertainment via the internet is taking over at every home. Some big companies are being seen as the traditional industries and consumer behavior, such as, Netflix,

Amazon, Airbnb, Uber and many many others. Thus, in case this will lead to an unstoppable and unlimited content that will be displayed and given without any boundaries and advertising will be effortlessly working around people making them unintendedly and automatically cope to this materialistic life.

Ecommerce over Conventional Shopping

Ecommerce will be predominant and taking over the purchases whether household purchases or business Due to the crazy increases in real estate, retails and rental prices. Autonomous vehicles will be used for shipping and orders of products. Thus, replenishment would be done automatically with a click of a button, which will lead to saving big companies tons of money, expensive shipping and expensive rents.

On the other hand, it is mentally healthier for people to be living better than before, since technology and innovation is considered an easily accessible tool that could make life easier. Only if it was taken to the extreme than it would leave humanity behind where humanity becomes pampered in comfort. For example: nowadays, people don't even bother themselves to leave the house or the office to get food or watch a movie, since food could be ordered online on such applications (Zomato, totters...) and movies can just be found and watched online within a click of a button on some easy use applications like: Netflix, PutLockers , etc... Thus, people should be aware of the coming change with their work environment which is one of the main issues that must be considered, where it could be also affecting businesses through the fast pace digitization than households. This could be a result of companies encouraging the new demanding technologies in order to empower themselves to be great competitors, save money and expenses and make their products and service more innovative and with a high quality.

Workforce

Nowadays, the biggest concern is the replacement of human beings and their labor with computers. In several ways, it is noticeable that the workforce has been affected by the digital age. The students that are recently graduating and the employees are meeting a huge competition global job market. Human would become useless and disposable where they could be outperformed if automation is recognized to be faster in doing human jobs in a more effective way. In the United States, for example, from January 1972 to August 2010, the sheer number of people who worked in manufacturing jobs fell from 17,500,000 to 11,500,000 while manufacturing value rose 270%.

The digital age and changes of life

Obviously, crafting and handwork will be less significant due to the presence of technology in this society which is hugely dependent on virtual data, web design, cloud computing and software development.

People would be working smarter in their life, by not taking the hard way for their work-life balance, especially people who are familiar with using software will find a better time to use their skills in order to automate their work, unlike those who will suffer the most with routine repetitive job cycles due to their menial works.

Agility and Competition

In this decade, everything only takes a click of a button, saving more money and more time for companies. In

addition, to the one-day delivery, the fast internet connection. All these could result in more profit which lead to greater growth and innovations which speeds lives.

It is not surprising that this life is impacted by all these technologies. So, it is normal to see companies and economies competing against each other over fast, delivery, quality, mass of production and quick services. Thus, receiving services is faster and easier these days. Moreover, what should be considered is that people are creatures of habit and the vision of the post digital era is still unclear and hazy. When the post digital ear shows its social and commercial advantages, then people might move to the opportunities it offers. However, cybersecurity is much appreciated in this digital ag, and its more prevalent in people's lives with the help of social media and search engines that possess people's data.

Seamless integration

The covert of silos into the center of excellence would be considered a major shift toward the digital age. Some companies are still working in silos to some extent. Some companies care about their unique functions when they have to, for example, their confidentiality but will still function within a holistic whole.

Technology will be a huge key that enables a cultural shift which is a part that is going to be involved, and some businesses will consider this shift significant. People will find it easier to communicate and share data by being provided with applications to talk to each other across functional areas.

The Uniqueness of the Internet

A. Increased Data Creation and Collection

In this disconnected world, it is clear that The Internet speeds up the pattern toward expanded data assortment. The information trail, known as conditional information, abandoned as people utilize the Internet is a rich wellspring of data about their propensities for affiliation, discourse, and trade. Conditional information, click stream information, or "mouse droppings," as it is then again called, can incorporate the Internet convention address ("IP address") of the singular's PC, the program being used, the PC type, and what the individual did on past visits to the Web website, or maybe significantly other Web destinations. This information, which might possibly be sufficient to distinguish a particular individual, is caught at different focuses in the organization and accessible for reuse and divulgence. A portion of the information created is crucial for the activity of the organization, similar to the telephone number that associates a calling party to the planned beneficiary, the IP address is fundamental, for without it the organization can't work. Be that as it may, different bits of information might fill needs past network activity. Alongside data purposefully uncovered through buying or enrollment exercises, this value-based information can give a "profile" of a singular's exercises. At the point when accumulated, these advanced fingerprints uncover the outline of a singular's life. This undeniably definite data is purchased and sold as a ware by a developing grouping of players.

B. The Globalization of Information and Communications

On the Internet, data and correspondences stream unrestricted across national borders. The Internet puts the corner store, and a store three mainland's away, similarly at the singular's fingertips. Similarly, as the

progression of individual data across public boundaries represents a danger to individual security, residents' capacity to execute with elements in different nations places individual protection in danger in nations that need security insurances. Public laws might be deficient, all alone, to give residents security assurances, across borders. Regardless of whether it is shielding residents from extortion, restricting the accessibility of unseemly substance, or ensuring protection, legislatures are tracking down their customary capacity to make and successfully implement approaches tested by the worldwide correspondence's medium.

C. Lack of Centralized Control Mechanisms

Effective monitoring of the generation, assortment, and stream of data for this tremendous scope might burden the assets of those as of now answerable for information security or different arrangements. While developing appropriate domestic policy might be adequate in a paper-based world or an incorporated and shut organization, where countries can handle the progression of data about residents subsequently shielding them from regions where assurance is lacking, data in an organized climate streams easy from one country to another, association to association, and strategy system to strategy system.

Conclusion

We hope that the situation might improve for the right to privacy, but the future appears bleaker. Since the advent of a digital society with online accounts, organizations that harvest user data have amassed tremendous powers. While certain merits can be argued for collecting user data, an equivalent responsibility remains to regulate and secure any stored personal data. Our identities are the most valuable thing we own. They are a form of wealth: identity capital. We should expect our identities to be protected from embezzlement and exploitation. Unfortunately, both staggering breaches of privacy take place and personal data is used for corrupt purposes. We would like to believe that infringements are rare and negligible, but we have all been victims of privacy invasion. Our identities are abused by companies who track customers to sell products, interest groups who manipulate social media to shape elections, and governments that seek omnipotent powers. Online businesses are often multinational and can hide between borders. Neither small organizations nor large governments can be trusted to restrict themselves. The right to privacy in the digital age demands a united, multinational alliance that will ensure all individuals in the world share an inalienable right to protect their identities. We urge the United Nations High Commissioner for Human Rights and international community to enforce accountability measures that ensure privacy invasions are monitored according to universal regulations. We must admonish governments who conduct indiscriminate mass surveillance and curtail their abilities to collect and utilize private information about individuals. We must penalize companies and individuals who steal our information or use it for illegitimate gains. While there are valid utilitarian reasons to enable minimal surveillance to enforce protective and punitive laws against heinous criminal activity, we must not allow individuals to become slaves of an oppressive system akin to George Orwell’s Big Brother. The UN must be proactive and provide a forum for those whose privacy is threatened. It is the responsibility of the international community to foster privacy-enhancing technologies that will protect all individuals equally. Regulations must restrict online entities from accessing all of our personal information. Unwitting

users should not be compelled into giving up their privacy or not having access to a technology. We must ensure that our data is not used without our knowledge or consent, nor for purposes that were not explicitly stated. Positive efforts are being made, but we are playing a game of catch-up.

References

- Asher, Jeff and Arthur, Rob. “Inside the Algorithm That Tries to Predict Gun Violence in Chicago”. The New York Times. June 13, 2017
- Flock, Elizabeth. "What Internet censorship looks like around the world". Washington Post. April 5, 2012
- Gutwirth, S. and De Hert, P. (2008). Regulating profiling in a democratic constitutional state. In Profiling the European citizen (pp. 271-302). Springer, Dordrecht
- Human Rights Watch. “China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent” November 19, 2017
- Tribunal Superior Eleitoral. “Biometria”. Setor de Administração Federal Sul (SAFS)
- UN General Assembly, the right to privacy in the digital age (A/RES/73/179)