Commission For Bonding, Promotion,
Diffusion & Social Communicatiom

NATIONAL SYSTEM
FOR TRANSPARENCY
ACCESS TO PUBLIC INFORMATION &
PERSONAL DATA PROTECTION

GUIDE FOR IDENTITY & DIGITAL CITIZENSHIP

Av. Insurgentes, Sur No. 3211, Colonia Insurgentes Cuicuilco, Alcaldía Coyoacán, Mexico City. CP 04530.

The opinions expressed by the authors were made in their personal capacity and do not reflect the institutional point of view of the National Institute for Transparency, Public Information Access and Personal Data Protection (INAI).

First edition October 2023

NST MEMBERS WHO PARTICIPATED

Norma Julieta del Río Venegas
Coordinator of the Permanent Commission for Bonding, Promotion, Diffusion and Social Communication with the NST and Commissioner of the National Institute of Transparency, Public Information Access and Personal Data Protection (INAI)

Luis Gustavo Parra Noriega
Coordinator of the Commission for Bonding, Promotion, Diffusion and Social Communication of the NST and Commissioner of the Institute of Transparency, Public Information Access and Personal Data Protection of the State of Mexico and Municipalities (INFOEM)

Adrián Alcalá Mendez
Commissioner of the National Institute of Transparency, Public Information Access and Personal Data Protection (INAI)

Josefina Román Vergara
Commissioner of the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI)

Amelia Lucía Martínez Portillo
President Commissioner of the Chihuahuense Institute for Transparency and Public Information Access (ICHITAIP)

Evelia Elizabeth Monribot Domínguez
Commissioner of the Institute of Transparency, Government Public Information Access and Personal Data Protection of the State of Hidalgo (ITAIH)

Francisco Javier Diez de Urdanivia del Valle
Commissioner of the Coahuilan Institute of Public Information Access (ICAI)

Julio César Bonilla Gutiérrez
Citizen Commissioner of the Institute of Transparency, Public Information Access, Personal Data Protection and Accountability of Mexico City (INFO CDMX)

Laura Lizette Enríquez Rodríguez
Citizen Commissioner of the Institute of Transparency, Public Information Access, Personal Data Protection and Accountability of Mexico City (INFO CDMX)

María de los Ángeles Guzmán García
Commissioner of the Transparency and Commission to Information Access of the State of Nuevo León (INFONL)

Naldy Patricia Rodríguez Lagunes
Commissioner of the Veracruzano Institute of Information Access and Personal Data Protection (IVAI)

Salvador Romero Espinosa
Commissioner of the Institute of Transparency, Public Information and Personal Data Protection of the State of Jalisco (ITEI)

NATIONAL SYSTEM FOR TRANSPARENCY
ACCESS TO PUBLIC INFORMATION & PERSONAL DATA PROTECTION

Commission for Bonding, Promotion, Diffusion & Social Communication

Xitlali Gómez Terán
Commissioner of the Morelense Institute of Public Information and Statistics (IMIPE)

Xóchitl Elizabeth Méndez Sánchez
Commissioner of the Office for Public Information Access, Transparency and Personal Data Protection and Good Government of the State of Oaxaca (OGAIPO)

Yolidabey Alvarado de la Cruz
Commissioner of the Tabasco Institute of Transparency and Public Information Access

COLLABORATORS

Adriana Yadira Cárdenas Tagle
General Director of Transparency, Public Information Access and Open Government
Editorial Coordinator of the Guiding Document

Anahiby Anyel Becerril Gil
Vice President of the Mexican Academy of Cybersecurity and Digital Law

Carlos Languendik Muñoz
President of Embracing Lives and Building Dreams, Civil Association

Erik Alejandro Cancino Torres
Professor of the Faculty of Communication Sciences of the Autonomous University of Tamaulipas

Guillermo Antonio Tenorio Cueto
Director of the School of Government and Economics of the Panamerican University

Héctor Guzmán Rodríguez
Director of the Personal Data Protection and Privacy Network at BGBG Firm

Iván Díaz González
Associate of the Mexican Academy of Digital Law

Javier Brown César
Public Ethics Specialist
Advisor in the Senate of the Republic

NATIONAL SYSTEM FOR TRANSPARENCY
ACCESS TO PUBLIC INFORMATION & PERSONAL DATA PROTECTION

Commission for Bonding, Promotion, Diffusion & Social Communication

EDITORIAL STAFF

Guide for Identity and Digital Citizenship

Introduction

Luis Gustavo Parra Noriega

The National System of Transparency, Public Information Access, and Personal Data Protection (SNT) since its consolidation as a coordination and deliberation body in charge of guaranteeing the exercise and respect of the rights of information access and personal data protection, has been responsible for providing and develop education and promotion of these two rights throughout the national territory.

Through the National Coordination, socialization efforts have been made whose importance permeates the most sensitive fabrics of our current society; for this reason, the SNT Entailment, Promotion, Broadcasting and Social Communication Commission, through its 2022-2023 work plan, proposed holding dissemination forums around the importance of digital citizenship; whose realization led to the need to jointly build a Guiding Document that allows us to generate collective knowledge with citizens so that they know in a more practical way, the implications and challenges of living in a digital society, generate awareness to be informed and understand the challenges and implications of living in a highly connected environment.

Thus, this document aims to explore key aspects that will lead us to build concepts of identity and digital citizenship with the help of experts, in the quest to highlight the importance that should be given to adequate digital education so that people can understand and responsibly use digital technologies.

This includes knowledge about online privacy, cybersecurity, responsible use of social media, and the ability to discern reliable information from misinformation.

In a digital society our personal data and privacy are constantly exposed, and it is precisely through them that we build our digital identity. In that sense, it is necessary to warn and know our digital and privacy rights, raise awareness about the importance of protecting our personal information and learn how to use it for our benefit.

Our data is so exposed and there is so much information available on the web, which means developing media literacy skills to be able to critically evaluate information, identify fake news and understand how digital media can influence our perceptions and opinions.

Regarding digital citizenship, keeping in mind the concept of "liquid society", which was coined by the sociologist Zygmunt Bauman to describe a society characterized by the lack of solid and stable structures, we can affirm in this context that digital citizenship refers to the rights, responsibilities, and behaviors of individuals in the digital environment.

Some challenges that arise in a digital society are the following:

1. Online ethics: It is essential to raise awareness about online ethics and encourage responsible and respectful behavior in the digital environment, considering the impacts of technology on human beings, even in such flexible and variable structures or situations of this type of society.

2. Citizen participation: Digital citizenship involves not only consuming online content, but also actively participation in civic and political debates and affairs. In a liquid society, where traditional structures may be less stable, it is important to

encourage online citizen participation and the use of technology to promote the common benefit.

3. Digital empowerment: Technology can be both a tool of empowerment and oppression. It is essential to raise awareness on how to use technology to promote positive social change and advocate for equality and justice to achieve effective digital citizenship.

Thus, the objective of this Guiding Document is to generate input for consultation and diffusion that allows generating useful public knowledge regarding identity and digital citizenship, since more and more aspects of our lives are developed online, from communication, search for information, demand for public services, carrying out online procedures, even financial transactions, so this document analyzes from the definitions, implications in early childhood, digital footprint, governance and the construction of digital citizenship.

I. FUNDAMENTS OF DIGITAL IDENTITY

Definition of Digital Identity

Francisco Javier Diez from Urdanivia del Valle

Currently it is almost impossible to find a person who does not have at least one account within the so-called "cyberspace social networks", although it seems redundant because the term "social networks" is practically only used to refer to said internet platforms. This implies new challenges and unexplored study spaces, or shallow in its essence.

One of these great challenges and little explored spaces, which has caused effects beyond cyberspace, is the one related to personality. This, due to its complex nature that represents a large spectrum of concepts according to the scientific vision from which it is approached, is fertile ground for the plurality of opinions on the matter, which open the door to individual visions rather than systematized schemes that seek the depth of its knowledge. With this in mind, we must understand that one of the ways to address the great challenges is to dissect them and analyze each element individually, which is why only the idea of identity and more specifically digital identity is necessary in the present.

Just as we all have an identity in the material world, to call the physical realm in some way, we all have that personal attribute that gives us an individual identity registered and recognized in cyberspace. In the material world, it is easy to recognize that institutional record that identifies a person, it may be before a governmental or religious institution, this depends on the social-legal system referred to, but it is relatively easy to follow the trail; however, the digital registry does not actually have an institution delimited by a clear social-legal system, but rather there are countless possible records with variables that address another concept that is little explored today, that of informational self-determination.

Also, in the material world it is easy to identify the social recognition of third parties compared to the identity of a person. There are many elements that make up identity, starting from the characteristic biological or physical elements, however, these elements do not properly exist in cyberspace, there everything is a construction of appreciation, since the structure that gives form is essentially a binary code that, thanks to great minds, we can all visualize it in a way that we easily recognize.

Although these elements of registration and recognition do not exist in cyberspace, as in the material world, every time the internet is used, a "digital identity" is built that allows the systems and people who operate them to recognize it practically. immediately and thus label us within a personalized identification classification. This leads me to a big question: Are we aware of what identity are we building in cyberspace? It is important to ask this and look for systematized paths that simplify walking, because, even if you don't want to, it is part of the "material identity" and, consequently, of the personality.

Beyond the awareness that is made of the identity that is being built on the internet, the reality is that it can be built or reconstructed as many times as desired, the difference at this moment is that there is the possibility of creating a "digital identity" consciously.

From this orientation guide, which allows us to have knowledge of what a "digital identity" is and its extent, one can be established that connects perfectly with what is intended to be obtained from the "identity of the material world." It is also possible to obtain the same registration identity, despite the multiplicity of registrations, and achieve a clear appearance of what we are and what we seek as people beyond delimited spaces.

Impacts of recognition of digital identity in early childhood towards digital citizenship

Adriana Yadira Cárdenas Tagle

Digital identity is an increasing relevant concept in our society, it has become an integral part of modern life and its impact on early childhood [1]is an issue that deserves our attention, given that it is progressively exposed to digital devices and online platforms, causing effects during the first years of life that will have an impact throughout our senior years, since this digital context is shaping their cognitive, emotional and social development.

First, it is important to highlight that digital identity refers to the image that a person projects online, through social networks and other digital media. According to Johnson (2018), digital identity can play a critical role in the early development of self-concept in childhood. Interacting with digital platforms allows them to explore, experience and share aspects of themselves that may not be as accessible in their physical environment. This capacity for digital self-expression contributes to the formation of your personal and social identity.

[1] In general, early childhood is defined as the initial stage of childhood, that is, that period of life through which people under 12 years of age go, in accordance with the provisions of article 5, both of the General Law of Children and Adolescents, as well as the Law of Children and Adolescents of the State of Mexico.

When we are observing the process by which children are aware of their online presence and are involved in activities in the virtual world, this can have significant impacts, both positive and negative, potentially affecting their development in different areas of their life.

One of the positive impacts is that it can contribute to the development of social skills and digital competencies. According to Mueller (2020), children who learn to manage their digital identity from an early age tend to develop a greater ability to interact and communicate in online environments. Furthermore, online interactions can promote social participation and empathy through contact with a diversity of perspectives (Subrahmanyam & Šmahel, 2011), which importantly implies that children who learn to master their strengths in digital spheres could effectively influence their environments as responsible citizens.

In this sense, it is the responsibility of the tutors in the first instance to be able to support the integration of technological aspects into the lives of minors, to insert responsibility strategies and limits in digital environments to avoid risk situations, however, the school authorities has a major challenge on how to migrate from being analog teachers to hybrid teachers, with the same tasks when having the in-person attendance of the students, but with a life to monitor in digital environments, for which to talk about ethics in digital environments, digital literacy and especially mental health of girls, boys and adolescents is the main area of opportunity that is seen so that they can develop a healthy digital identity.

As I mentioned, there are risks and dangers associated with the recognition of digital identity in early childhood, such as premature exposure to social networks and digital identity can increase children's vulnerability to bullying, cyberbullying (Smith, 2019), by having an early digital footprint, children could face difficulties controlling their private life later, since their personal information will be available online and furthermore this could cause negative implications in the exercise of their rights, from apply for certain schools, get a job and even affect their political electoral rights.

To address these challenges and take advantage of the benefits of digital identity in early childhood, it is essential that mothers, fathers, educators, and especially society as an information bridging gear, have a balanced approach that encourages the positive and responsible use of digital identity technology while we are aware of the possible risks and benefits that come with the early consolidation of a digital identity, about which we should ask legislators in these cases how the right of cancellation or the so-called right to be forgotten that in Mexico has caused so much controversy will act.

It is necessary to make this type of approach as every day there is a considerable increase in girls, boys, and adolescents online, who are forming their digital identity, and who are already prey to the companies that little by little will be able to "form" their preferences, in minors and that possibly sometimes is not for adequate decision making; that is why it would be worthwhile to have a network for creating and verifying content specifically for minors, as well as encouraging access throughout the design on platforms and browsers.

It is not enough to promote solid digital educational strategies and the adoption of clear guidelines maximizing the benefits and minimizing the dangers, but rather the connection with civil society is essential to achieve adjustments and controls that lead early childhood to consolidate themselves as the most prepared citizens of the time, more aware, capable, and empathetic, competent of ensuring that the sustainable development objectives are met.

References

- Johnson, T. (2018). *The Impact of Early Exposure to Digital Identity Formation in Early Childhood.* Journal of Children Development Studies.
- Law of Children and Adolescents of the State of Mexico. (2015). Legislature of the State of Mexico. Obtained from: https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig098.pdf
- General Law of Children and Adolescents (2023). Chamber of Deputies. Obtained from: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGDNNA.pdf
- Mueller, L. (2020). *Digital Identity and Social Skills in Early Childhood: A New Perspective.* Journal of Early childhood Development.
- Smith, J. (2019). *Risks and Dangers of Early Digital Identity Recognition in Early Childhood.* Cyberpsychology Review.
- Subrahmanyam, K., & Šmahel, D. (2011). *Digital youth: The role of media in development*. Springer.

Analysis of the construction and management of digital identity

Julio César Bonilla Gutiérrez

As society becomes more digitalized, personal digital identity becomes a fundamental extension of our being. This essential component of our online interaction poses both opportunities and challenges in its construction and management that, in many ways, falls on us.

Digital identity includes the set of online characteristics, data and information that represent and define an individual or entity (van Dijck, 2013). This includes: i) Personal data: such as name and date of birth; ii) social network information: profiles and publications; iii) transaction history: purchases and bank records; and iv) online behaviors: websites visited, and applications used.

The construction of digital identity

Authenticity versus construction. The dualistic nature of digital identity is torn between authentic representation and deliberate construction (Boyd, 2010). People tend to:

- Model their identity: Presenting an idealized version of themselves.

- Control your narrative: Carefully deciding what to show and omit.

- Interact strategically: Adapting to the norms and expectations of specific platforms.

However, the way we model and construct our digital identity has tangible repercussions; for example, in our reputation, because online perceptions can affect our offline opportunities. Also, because digital overexposure can lead to security risks. Another important element that we must consider is our mental well-being because digital representation can influence our self-image and self-esteem.

Challenges in digital identity management

Due to the above, there are various challenges that are related to people's digital identity and that are not, in any way, irrelevant. For example, we have the same in terms of security and privacy because, as the threat of cybercrime grows, protecting digital identity is crucial (Deuker, 2011). It is essential to engage robust authentication mechanisms, limit the disclosure of sensitive data and be vigilant to potential online threats. The tension between reality and representation can be mentally challenging (Turkle, 2011). It is therefore vital to recognize and address digital fatigue, encourage honest representation online, and seek support when the pressure of digital identity becomes or may become overwhelming.

In the previous context, there are invaluable opportunities that can be taken advantage of; for example, education is essential to train people to manage their digital identity effectively and securely (Hargittai & Marwick, 2016). Likewise, emerging solutions such as blockchain promise to revolutionize identity management (Tapscott & Tapscott, 2016).

On the citizen empowerment side, controlling our digital identity can enhance civic participation and our informational self-determination in cyberspace.

Our digital identity, although intangible, has very real consequences. Navigating its complexities requires both technical understanding and self-awareness.

References

- Boyd, D. (2010). *Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications*. Routledge.
- Van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media.* Oxford University Press.
- Deuker, A. (2011*). Identity Management for e-Service Ecosystems*. University of Stuttgart.

- Hargittai , E., & Marwick, A. (2016). *The Life Cycle of a Social Media Meme.* Cambridge University Press.
- Tapscott, D., & Tapscott , A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* Penguin.
- Turkle, S. (2011). *Alone Together: Why We Expect More from Technology and Less from Each Other*. Basic Books.

Importance of personal data protection (violations)

Norma Julieta del Río Venegas

The personal data protection is an issue of major relevance with the arrival and evolution of the technological environment with which we live, where information from individuals is collected and stocked, which stores sensitive data that, if it falls into the wrong hands, can put at high risk to their owners.

Today, this technological advance forces us to provide our personal information, both to private services such as applications and service provision, as well as on government platforms. We must understand privacy as a sphere that is not public and to which third parties should only access with our full consent, since it is a space that contains personal data that only its owner knows.

What is a personal data breach?

It is an information security incident that affects personal data at any stage of its processing, however, let us remember that all breaches are information security incidents, but not all security incidents are considered breaches.

Obligations established by the General Law on Personal Data Protection Held by Obligated Subjects (LGPDPPSO) that the proprietary areas must comply with regarding violations. (Chamber of Deputies, 2017)

- Analyze the causes why the violation occurred and include the security document, preventive, and corrective actions in your work plan (Article 37).
- Keep a log of violations (Article 39).
- Inform the owner and the INAI of violations that significantly affect the economic or moral rights of the owner (Article 40).

Types of breaches

- Loss or unauthorized destruction
- Theft, loss, or unauthorized copy
- Unauthorized use, access, or processing
- Damage, alteration, or unauthorized modification
- Unauthorized disclosure or disclosure

Guiding principles of personal data protection. (INAI, 2019)

The treatment that must be followed by any person who uses personal data, including the communication environment to ensure the non-infringement of personal data.

- Legality and loyalty, consent, information, proportionality, purpose, quality, and responsibility.

For the INAI, the handling of personal data related to the identity of a person, as well as the processing of other data collected, requires the greatest possible care from the regulatory sphere in force in our country, since any affectation or violation could generate significant damage that is difficult or impossible to repair, especially considering that personal data refers to aspects that allow a person to be uniquely associated and identified and, therefore, constitute irreplaceable characteristics.

It is essential that the processing of personal data complies with the principles, duties, rights, procedures, and obligations provided for in the regulations regarding the protection of personal data, thus complying with the General Law of Personal Data Protection Held by Obligated Subjects and with the Federal Law of Personal Data Protection Held by Private Parties.

References

- General Law of Personal Data Protection a Held by Obligated Subjects. (2017). Chamber of Deputies. Obtained from https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf
- Competency frameworks. (2019). INAI. Obtained from https://micrositios.inai.org.mx/marcocompetencias/?page_id=370

Risks for digital identity: digital violence, some types and examples.

Xitlali Gómez Terán

With technological advances that, without a doubt, represented a series of benefits for society, they were also accompanied by various risks, including digital violence. The INEGI (2022) indicated that internet users (104.2 million Internet users aged 12 and over) victims of cyberbullying increased [2]from 21% to 21.7% in 2021 with a higher prevalence in the case of women (22.8%) than men (20.6%) and that the most frequent situation was contact through false identities (INEGI, 2022).

The National Institute of Statistics, Geography, and Informatics (INEGI) (2022, p.1) carries out a measurement through the Module on Cyberbullying (MOCIBA), which explores various expressions such as:

[2] *(...) refers to the situation in which someone is exposed, repeatedly and for a long time, to negative actions by one or more people who seek to harm or cause inconvenience. The means they use are electronic, such as cell phones and the Internet. INEGI, 2022, p. 1*

i. Receive offensive messages, with insults or ridicule.
ii. Receiving offensive calls, with insults or ridicule.
iii. Being criticized for your appearance (way of dressing, skin tone, weight, height, etc.) or social class.
iv. That a person impersonated you to send false information, insult or attack other people.
v. Being contacted using false names to annoy or harm you.
vi. Be monitored on your sites or accounts on the internet to cause you annoyance or harm.
vii. Being provoked online into reacting negatively.
viii. Receiving sexual advances or proposals that bother you.
ix. You received photos or videos of sexual content that bothered you.
x. Publish or sell real or simulated sexual images or videos of you without your consent.
xi. Post personal information, photos, or videos to harm you.
xii. Threaten to publish personal information, audio, or video to extort; and
xiii. Another situation that has affected you. (INEGI, 2022, p. 1)

The consequences that may arise from violence depend largely on the characteristics of the person affected; but in general terms, digital violence can translate into violent behavior in the real world such as physical and sexual violence, which can even lead to the death of the person. Likewise, it can lead to victims starting self-harming behavior and the impact can be so serious that it can even lead to suicide. In the case of adults, they may lose their job, their personal and professional reputation may be affected, and their project in the public sphere may be canceled by the United Nations Population Fund (UNFPA, 2022).

Any person who interacts in the digital sphere can be a victim of violence in cyberspace, however, this can worsen when they belong to historically discriminated groups such as women, LGBTIQ+ community, people of color, people with disabilities, among others. Hence, this type of behavior comes from misogyny, racism, and homophobia.

Special relevance deserves the attention that must be paid to children and youth who participate in the digital world, who have greater exposure because they spend more time on the internet, are unaware of the means to protect themselves and the consequences of digital violence. It can cause serious damage and limit its full development.

References

- INEGI (2022), Press Release No. 364/22, July 13, 2022. Available at: www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf
- UNFPA (2021). Guidance document for reporting on digital violence: Practical reference guide for journalists and media, Available at: https://www.unfpa.org/es/resources/Documento-orientativo-para-informar-sobre-violencia-digital

Tips to protect digital identity and maintain online privacy.

Iván Diaz Gonzalez

Before starting with any advice regarding how to protect identity, it is essential to analyze the construct of digital identity. Identity by itself is not a finite element, since, depending on the context, place and interactions, it will address a set of elements that will allow the identification of an individual in a finite space-time, hence identity must be taken as a set of (identity) components, which allow an individual or entity to be distinguished from the rest of the entities that are in the same space-time. These identity components are based on physical, psychological, documentary, procedural, and operational characteristics behavior.

When the topic of digital is addressed, the context of whether identity will be used in electronic media or any other technology is commonly addressed, however, I want to address that beyond the use of a technology, the digital topic creates a space-different time in a domain of operation called cyberspace that, although it runs parallel to physical space-time, in cyberspace we can find a larger number of tools to modify the context, since the place is not clearly defined as there is no territory delimitation and interactions can be altered from time to time.

Once the definition of digital identity has been contextualized, I want to highlight that in order to carry out identity protection it is not enough to simply buy a set of tools, buy software for managing credentials, save and learn my passwords or do not allow cookies, for the protection of identity a great commitment is required from each of the individuals, hence it is proposed that the entities from which their identity is required to be protected must comply with a set of controls that will allow them to align the protection efforts in a manner appropriate to the needs of the entity, its context and the set of identity components.

For this protection, it is recommended to follow 4 simple steps that are described in the identity theft protection framework also called KAOS (acronym for words in English referring to knowledge, assessment, organization, and security) (Identity Management Institute, sf). From this point of reference, it follows that the first thing we must do to take care of our identity is to know what components of my identity I have and where these components are distributed, for which it is important to have an inventory of all the components and know to whom or to whom that we have shared these components with you.

The next step is to assess the treatment of the components of the identity and to do so it is necessary to evaluate whether each of the components that have been delivered to third parties are justified in their treatment, if they are being treated correctly, what the components are updated and thus clarify each of the deliveries and elements of the identity component inventory.

Since we have a clear inventory, the next thing is to categorize the information, which can be done by protection priority or by importance within the context; regardless of the way of categorizing it, from this process an order can be obtained that will allow not only to have control of the components of the identity that are in the possession of the entity but also with third parties, which will allow the monitoring of the movements that they are carried out with the components of identity and thus be able to act just at the time when the information could potentially be put at risk and know what to do.

Finally, security controls must be implemented, such as limiting access to information in space-time, not sharing identity components with any person or entity, not connecting to sites that are dubious in their processes, as well as any other control process that makes you feel that your identity information is in an acceptable state of processing and security.

In conclusion, digital identity can be protected with the effort of each person through adequate control of its identity components and establishing interaction with each of the people, entities or sites with which information is shared.

References

- Identity Management Institute. (sf). *Identity Management Institute center for Identity Governance.* Retrieved from *https://identitymanagementinstitute.org/kaos-identity-theft-protection-framework/*

Tips to protect digital identity and maintain online privacy.

Xitlali Gómez Terán

To prevent the risks of identity theft or misuse of social media accounts, as well as cyberbullying, according to the service provider UANATAC[3] (2020), it is important to implement the following measures:

1. Update software regularly: keeping our equipment and applications updated is one of the factors that strengthens security and prevents the attack of new computer viruses.

[3] International company expert in digital identity, belonging to the Bit4id business group, which was born with the vocation of generating value and trust in digital transactions.

2. Be careful when browsing the internet: check the links before clicking on them, especially with fake news (the famous " fake news ") that have become a frequent method of carrying out cyberattacks.
3. Browse only on safe sites: avoid providing personal data until verifying the security level of the portal. The indication "https" before the URL indicates that it is a secure connection, protected by encrypted technology.
4. It is important to be up to date on cybersecurity measures: cybersecurity experts discover new methods to protect the personal data of internet users.
5. Use Wi-Fi connections protected by WPA encryption: avoid wireless networks such as those offered in public places, as it can leave your data exposed.
6. If you face digital harassment through social networks, there are various resources; for example on Facebook[4] they have resources that can help, Twitter [5], as well as Instagram[6] and TikTok[7]. (UNICEF, s/f).

References

- UANATACA, six tips to protect it. Available in:

https://web.uanataca.com/es/blog/transformacion-digital/proteger-identidad-digital

[4] https://www.facebook.com/safety/bullying

[5] https://help.twitter.com/en

[6] https://about.instagram.com/es-la/safety *and* https://about.instagram.com/es-la/community/anti-bullying

[7] https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-video *and* https://www.tiktok.com/safety/es-es/bullying-prevention/

- UNICEF (2020), Cyberbullying: What it is and how to stop it. Available at: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Digital Footprint

Laura Lizette Enriquez Rodríguez

The use of the internet today has become one of the most common activities for people, so much so that there is currently talk of the generation of a digital identity, derived from the set of information about us online, which translates into "the set of attributes that link a personal entity with its online interactions" (Álvarez, 2018); That is to say, after our time on the internet, an image or reputation is created that is fed by the data we put there.

Thus, all the activities we carry out on the networks generate a digital footprint, a trace that we leave every time we access the Internet and that can provide benefits in our daily lives but is also related to concerns about privacy and risks associated with of our personal data protection.

From information that we share on the pages we visit, about the products we buy, our location, work, academic information, and our personal relationships, to identification through our IP address that allows our device to be recognized uniquely on the internet, among many more, constitute a more complex network, identifying us as users and thus forming our digital identity.

Likewise, what we post on social networks like Facebook, on LinkedIn, what Google says about us and what in the medium or long term creates a reputation (e-reputation) about us in the virtual sphere.

It is important that, as users, we know that this digital footprint can be created directly or indirectly, that is, by ourselves being the ones who voluntarily share our information or that generated by third parties.

Specifically, the digital footprint is generated directly when we as internet users are aware of creating a trace on certain sites, such as when we voluntarily leave our credit or debit card information, when we accept the privacy notices of the sites we visit or when we enter our emails into them.

On the contrary, the indirect way occurs when, even without our knowledge, internet pages or social networks are saving data about us, such as search histories, recent activities, or sites we visited.

As a result, our digital footprint generates what is known as "bubble filters," which predict and select the information that the user might be interested in, adjusting to our preferences based on our personal information.

However, when faced with these filters, information is generated that is outside our will, so our perception of the information sought, the constructed ideology and even our own digital identity could be biased by the delimited universe of results returned by the filter, generating as a negative consequence, possible manipulation, and misleading advertisements, as well as the lack of freedom to access a larger amount of content.

In this context, the ideal would be to reach what Christopher Allen calls "sovereign identity", that is, the next step of digital identity, in which the owner has absolute control of their personal information.

References

- Allen, C. (2016). *The Path to Self-Sovereign Identity.* Coindesk. Available at: https://www.coindesk.com/path-self-sovereign-identity
- Álvarez, C. (2018). *Digital identity: What is it and how to protect it?* Financial Regulation. BBVA Research. Available at: https://www.bbva.com/es/identidad-digital-protegerla/
- Pariser, E. (2017). *The filter bubble: how the web decides what we read and what we think.* Spain: Taurus.

What is a digital footprint and how is it generated?

Naldy Patricia Rodríguez Lagunes

Almost all activities of daily life are related to the use of Information and Communication Technologies (ICT). When people are browsing, using an electronic device to visit websites, interact in applications, forums, and files, they leave data traces. These data traces constitute your digital footprint.

This digital fingerprint can be a useful tool for those who want to investigate people's online activity, as well as obtain data about their electronic devices.

It should be noted that a footprint alone does not make much sense if we look at it in isolation, that is, if we compare this to a crumb of bread (a data point) it does not reveal much, but when considered as a set of footprints, through a compilation of these, we can obtain the largest network of personal data that exists, since we would have a detailed history of the people, including the web addresses they visit, the searches carried out, the texts they send, as well as like the photos and files you upload and download, therefore, if a person uses the internet, they cannot help but leave a digital footprint.

How long does a digital footprint last? Its duration will depend on the surface where it is printed; if the footprint is stamped on concrete (photos or videos uploaded to the Internet) its duration will be much longer than a footprint drawn on sea sand (search or browsing history), so it is the responsibility of each person to take care of it, your digital footprint, as this forms the basis of your online reputation.

It should be noted that there are two types of footprints, passive and active, distinguishing one from the other by the informed consent of the people.

Thus, when people carry out data exchange activities online intentionally or with consent, this will form their active digital footprint, such as: filling out forms, their publications on social networks, the use of their email, among others; while the passive footprint will be that which refers to the data collected when your online activities are tracked without your consent, such as, for example, data on the use of websites (how many times you visit a website, IP address, how you reach a website), financial records, etc.

In short, our digital footprint could be used to evaluate the type of person we are, for better or worse. No matter how anonymous it may seem, what we do on the internet is passively monitored and recorded.

Although it is not predictable when our data will be used for a scam or identity theft, the dangers that come with having a digital footprint, without knowledge of what it entails, can be disastrous if it is misused, for example by doxing, which is defined as the practice of publishing personal information of third parties with the intention of intimidating, extorting or otherwise affecting (Lameiras). This is done by revealing identifying information about a person online, such as their real name, address, place of work, financial data, telephone number and any other personal information.

For this reason, " *a digital footprint could be considered sensitive if through improper use of it one can have access to privileged information that could put at risk the security or patrimonial or financial stability of a person or even their legal status."* In conclusion, our digital footprint is as important as our personal data since it constitutes our digital identity.

References

- Amor, JR, Villegas, C. (2022) *Digital footprint: servitude or service?* Tirant Humanities Publishing House. Valencia.
- Ibañez, R, (1989) *The digital footprint and Mexican law.* Mexico, DF: Sista.
- National Institute of Transparency and Access to Public Information (INAI) (2018) *Guide for the Treatment of Biometric Data.* Mexico City. https://home.inai.org.mx/wpcontent/documentos/DocumentosSectorPrivado/GuiaDatosBiometricos_Web_Links.pdf
- Lameiras , L. (2022) What is doxin and how to protect ourselves? News, opinions and analysis from the ESET security community. Obtained from: https://www.welivesecurity.com/la-es/2022/09/16/que-es-doxing/

- Maldonado Fabián, NI (2021). Fingerprint - UNAM Central Library. available in the following electronic link: https://www.bibliotecacentral.unam.mx/index.php/desarrollo-de-capacidades-informativas-digitales-y-comunicacionales/huella-digital

Awareness about the importance of taking care of your digital footprint and how it affects online reputation.

Miriam Josefina Padilla Espinosa

When a user makes a publication on their social networks, provides a comment on a video, uploads a photograph, or tags the places they frequently visit, they generate information that is available on the internet and provide details about the different activities they carry out on this site.

It is important to know that this information can be generated and consulted by the user or by third parties and that the set of this data generates a digital reputation that is important to take care of, given that it becomes the first contact that unknown people will have about the user person.

In some cases, this information can be decisive in whether to provide academic support or a professional opportunity and is also used by companies that, based on the information from the fingerprint data, create profiles of users that can be marketed with other companies.

Some ways in which companies collect data from users on the internet are through “cookies”, which are small files that are stored on their devices and that contain information about navigation, the ads they have viewed, the time zone, geographic location and even passwords.

Given the type of information that is stored in cookies, its protection is important considering that cyber criminals can carry out illicit actions to obtain it, such as: session theft or hijacking, redirecting to fraudulent online stores or exploiting vulnerabilities in computer programs or in the browser.

Additionally, this footprint information can be used by attackers to collect data about the user that can be useful to carry out more effective social engineering attacks.

Therefore, it is of utmost importance that users know what information about them is available on the internet, this will allow them to know what privacy and security settings need to be reviewed and strengthened, for this they can consult different guides and recommendations.

In addition, users can use navigation in incognito mode so that the browser will not store any type of information about the web pages visited.

Another important recommendation is to analyze whether the authorizations provided to sites to collect cookies are permanent or temporary.

It is essential that users raise awareness about the importance of knowing and protecting the information that is available to them on the internet and promoting the culture of reporting to report those pages that expose personal information without their consent.

References

- Spanish Data Protection Agency. (2019). *Internet privacy and security guide.* AEPD. https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-y-seguro-en-internet.pdf
- INCIBE. (2018). *Between cookies and privacy.* INCIBE Citizenship Blog. Recovered from https://www.incibe.es/ciudadania/blog/entre-cookies-y-privacidad
- Ministry of Justice and Human Rights of the Nation. (s/f). *What is digital fingerprint on the Internet?* Calls on the Web - Situations. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-huella-digital-en-internet
- UNICEF (2020). *Guide on Digital Coexistence.* UNICEF Argentina. https://www.unicef.org/argentina/media/9481/file/Gu%C3%ADa%20sobre%20Convivencia%20Digital-2020.pdf

II. RESPONSIBLE DIGITAL CITIZENSHIP

Definition of digital citizenship

María de los Ángeles Guzmán García

The concept of digital citizenship is increasingly present in the discussion of public policies and the academic world, so to talk about digital citizenship it is first necessary to understand what is meant by this concept; UNESCO defines it as a set of competencies that empower citizens to access, retrieve, understand, evaluate, and use information for creative purposes.

From this definition, it is important to highlight that digital citizenship refers to the set of rights, competencies and obligations that allow people to use, freely and responsibly participate in digital technologies, allowing them to understand, navigate, participate, and interact between the civil society and government in an ethical and safe manner.

Cyber citizenship is part of the electronic government system or digital democracy, which consists of the administration of State resources through new technologies, to make life easier. Likewise, it streamlines various procedures and services provided by the government, as they are carried out electronically from any place with Internet access; for example, requesting birth certificates, CURP, cadastral procedures, complaints to the prosecutor's office, among others.

In terms of access to information and protection of personal data known as ARCO rights [8], it is important to note that these can be exercised through digital citizenship, through the National Transparency Platform (PNT), implemented since 2016, in the that people can exercise their rights, requesting public information of general interest, as well as requesting access to personal data protected by public institutions.

Digital citizenship brings with it the benefits of speed in government procedures without leaving home in real time, greater participation in making complaints and contact with authorities. Another way is access to digital education through information and communication technologies (ICT), which help to train critical people, aware of the use of these technologies and the risks, as well as their benefits and possibilities. All of this greatly increases comfort and improves people's quality

[8] Access, Rectification, Cancellation and Opposition .

of life, as well as reducing travel times, in those that were previously carried out in person.

But not everything is ideal when using digital media, for example, in the educational field, during the COVID-19 pandemic, the lack of an efficient digital infrastructure by Mexican universities and many other places in the world was demonstrated, to carry out classes through safe and effective electronic means. This was solved thanks to quick action by the university authorities, these deficiencies were corrected, achieving the delivery of online education in a safe, transparent, and private manner.

On the other hand, although technology has advanced by leaps and bounds, there are still areas of opportunity, such as inequalities in internet access among vulnerable groups in Mexico, which are determined based on economic, cultural, geographic, and gender criteria, age, etc.; since not all citizens have physical access to telephone and internet, this despite the fact that today they are considered basic human services.

Another risk is the generational digital divide, mainly due to age, which refers to the distance between those who use technologies as part of their daily lives and those who do not have access to them, or who, even if they have it, they do not know how to use them. This occurs in many cases, because most of the population over approximately 55 years of age does not have skills or abilities in the digital world.

The absence of public policies, digital privacy regulations, as well as the lack of adequate regulation of the right to one's own image, honor, and cybersecurity, represents a danger for citizens; since private life can be irremediably affected if relevant measures are not taken in time. In Mexico there is no effective and homogeneous regulation that protects privacy, since there are only laws and regulations regarding personal data protection, and the content of these rights is different.

In our country, particularly in Mexico City, through its Constitution the right to one's own image is regulated, in its article 6, section c) numeral 1, which establishes that every person, group or community has the right to a name, to its own image and reputation, as well as to the recognition of its identity and legal personality.

There are legislative advances of great importance and evolution of the law such as the Olimpia Law, consisting of a set of legislative reforms to local criminal codes, which recognize digital violence as a type of crime and is punishable with financial fines or prison sentences for those who violates people's privacy through digital media. However, Mexico still does not have the sufficient and necessary regulations for the protection of rights regarding digital technologies.

It is necessary to produce a legislative framework of regulations aimed at providing guarantees to citizens regarding the protection of their personal information on digital platforms, so that people can use technology in a safe and protected manner. To do this, it is necessary to promote safe practices and behaviors in the use of digital tools. This can only be achieved with the implementation of public policies and legislative work. Likewise, a culture of awareness and Broadcasting must be promoted to promote information protection program and their rights, as well as basic technological knowledge.

References

- INAI (2017). National Transparency Platform. Available at: https://www.rendiciondecuentas.org.mx/wpcontent/uploads/2017/06/SAI_INFOMEX-Y-PLATAFORMA-NACIONAL_FINAL-5_Junio.pdf (accessed September 11, 2023).

- INEGI (2022) National Survey on availability and use of information technologies in homes (ENDUTIH) 2022. available at: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22. pdf (Accessed September 11, 2023)
- Morduchowicz, R. (2020) Digital citizenship as public policy in education in Latin America. UNESCO Website: https://unesdoc.unesco.org/ark:/48223/pf0000376935
- Supreme Court of Justice of the Nation. (2011). Production and Services. The reasons used by the Legislator who reformed and added the Relative Special Tax Law, effective as of two thousand ten, are reasonable to justify the tax on Telecommunications Services and to Exempt Internet access. Judicial Weekly of the Federation. Available at: https://sjf2.scjn.gob.mx/detalle/tesis/162316

Citizenship and Digital Identity: Protecting privacy in the virtual world

Josefina Roman Vergara

In the digital age in which we live, citizenship and digital identity have become fundamental concepts that deeply impact people's lives. Global interconnection and increasing dependence on technology have given rise to new ways of interacting, communicating, and participating in society.

However, this advancement has also brought with it challenges regarding the privacy and security of our personal data. In this text, we will explore citizenship and digital identity, the most relevant recommendations to protect privacy in the digital environment, as well as the best global practices aimed at guaranteeing people's digital rights.

Citizenship and Digital Identity: Definition and Meaning

Digital citizenship refers to the active and responsible participation of individuals in the digital world. Just as in the physical world, where citizens are part of a society and have rights and responsibilities, in the digital environment, people are also part of an online community and must assume similar responsibilities. Digital identity, for its part, is made up of the information that a person shares online, including personal data, social media activities, and more.

Bill of Rights of the Individual in the Digital Environment. Good Practice Code

In a world where online interactions are increasingly frequent and digital transactions are commonplace, citizenship and digital identity are essential aspects of modern life. Digital identity can affect how we are perceived by others, our job opportunities, our social relationships, and more. Therefore, it is crucial to consider how to protect our privacy in this context.

Citizenship and digital identity are key aspects of our contemporary life. As we participate in the digital world, it is essential to take steps to protect our privacy and security.

In this context, on August 21, 2023, the Data Protection Commission of the National Transparency System, prior to the opinion of civil society, experts, and the Federal Telecommunications Institute, approved the "Bill of Rights of the Individual in the Digital Environment: Good Practice Code".

This document represents a joint effort to disseminate the rights that any internet user has, as well as the good practices that public and private institutions could implement.

It should be noted that this document does not have binding effects, since, as has been said, we do not pretend to be legislators; rather, it points out the basic rights for the development of the digital person and for them to fully achieve the performance of many daily activities, whether leisure, work, administrative tasks, etc. and, on the other hand, it points out the obligations that the State must assume and the good practices that organizations could implement to guarantee these rights.

This Bill helps us visualize and create awareness and understanding of the impact and consequences of digital environments and spaces, adapting the human rights recognized in the Universal Declaration of Human Rights, the Political Constitution of the United States of Mexico and international treaties and agreements, those of which Mexico is a part, to the environment of the digital world.

It is therefore necessary and urgent that all actors and voices in the digital environment develop fully in this context, but at the same time assume commitments and obligations for harmonious coexistence. Thus, the purpose of this Bill is to provide a code of good practices, adjusted to the framework of international Human Rights for the compliance and advancement of Human Rights in the online environment.

The Bill is made up of 9 chapters, namely, Digital Equality, Digital Environment Liberties, Social Security Rights and Personal Protection Data, Rights to Participation, Democracy and Good Digital Government, Rights of People in Vulnerable Situation, Neurorights, Ethics in the Use of Artificial Intelligence, and Defense Media and Rights of Cybercrime Victims, Digital Violence and Human Rights Violations.

In short, with this document, Mexico constitutes itself as one of the precursors of the conversation about digital rights, in the face of interconnectivity and the accelerated use of information technologies.

Digital citizenship, rights and responsibilities

Guillermo Antonio Tenorio Cueto

In her wonderful book "Privacy is Power", Carissa Veliz answers a question that was raised many years ago with the accelerated advent of new technological developments about whether privacy still existed. For her, it continues to exist and must be defended under the new digital ecosystem. And today, it seems, there is not a corner of our lives that is not susceptible to capture by digital environments. The reader thinks about sleep measurements with smart watches or the times when you clean the floor of your house with a robot vacuum cleaner. It seems that all human life is called to be converted into data that profiles us, segments us, and predicts our behavior.

Is this process inevitable? I think so. In the next 10 years we will observe deeper transformations associate to the so-called metaverses of immersive reality where the so-called internet of the senses or emotions will be an everyday reality. Trying a Colombian coffee (without actually trying it), living the experience of a World Cup final (without actually being in it) or climbing a mountain (without sweating and fatigue included) will increasingly take over our routines, distancing human beings from the experiential reality to immerse you every day in a virtual reality where everything is measurable, everything is predictable and where without a doubt, sensations, reactions and emotions will be measurable within the system.

All the cases narrated have a common denominator which is the obtaining, handling, transfer, and data storage. In this sense, it is pertinent to assume that in the digital age our behavior must be directed by digital responsibilities. This implies not only being aware of who we share our data with, adequately informing myself of their processes, but also respecting the privacy of others and of course knowing how to reject data capture processes when they are clearly disproportionate or abusive. This is where the so-called digital citizenship begins to be cast.

Its profound responsibility implies for all of us the obligation to be duly informed of the processes carried out by all organizations that process data emanating from our private lives. Properly informing ourselves of the terms contemplated in a privacy notice is no longer an exercise from which we can evade, but rather constitutes the ideal mechanism to abandon victimization in the processing of data. It is also necessary that this digital citizenship be strengthened by establishing the measures we take to protect our information from possible attacks or breaches. The naivety of years past no longer has a place within a true digital citizen.

Private life, as a right, is a choice that entails its expansion or weakening. It is up to each of us to make that choice. Full knowledge of what will happen to our personal information necessarily enables the possible means of defense that we will have if it is violated, mistreated or shared illicitly.

Digital citizenship means knowing and exercising my rights linked to the development that each of us have in digital environments.

Building digital citizenship based on healthy management of the information we share, allows us to expand its horizons to other areas of human behavior in those environments, since it is derived from the awareness that prevention and reaction to mismanagement of information entail. information, we can build a responsible digital image in all its facets. The person who assumes, practices and lives this, can relate in a timely manner, based on the health care they take of the information they share online. In other words, ethics in digital behavior is built from the way in which we relate to our information and is projected into the way in which we relate to the information of others.

Without awareness in all of this, it will be difficult for us to move towards solid digital citizenship.

References

- Castellanos, J. in Arellano Toledo, Wilma (2022) Right to privacy and right to information from a comparative perspective, Tirant lo Blanch, Mexico.
- García, D. (2022) Freedom of expression 4.0 in the system of the Human Rights Convention. Tirant Lo Blanch, Valencia.
- Quijano, C. (2022) Right to privacy on the Internet. Tirant lo Blanch, Mexico
- Tenorio, G. (2022) Let's assume digital citizenship, El Economista. Consulted at: https://www.eleconomista.com.mx/opinion/Asumamos-la-ciudadania-digital-20220624-0033.html. Last visit on October 1, 2023.
- Veliz, C. (2021) Privacy is power, DEBATE, Spain.

Key aspects of digital citizenship: respect, ethics, and online civic participation.

Evelia Elizabeth Monribot Dominguez

Today's society is characterized by being dynamic, highly technological, focused on information, knowledge, and communication, but on the opposite side it shows fragile ties, constant changes, and lack of stable values, which is reminiscent of Zygmunt Bauman's concept of liquid society. This scenario requires that a citizen have basic skills such as learning to solve problems, decision making, knowing how to communicate and participation.

According to UNESCO, digital citizenship is made up of a set of skills with which users can "access, retrieve, understand, evaluate, and use, create, and share information in a critical, ethical and effective manner to participate and engage in personal, professional and social activities". Furthermore, it is not enough to be connected to the internet, but it implies having the skills to know how to navigate the web and use it responsibly.

There are native people and digital immigrants. Marc Prensky defines the first ones as those who are immersed in technology and were born with it, and immigrants are those who find it more difficult to adapt to the digital world.

In continuation with UNESCO's conceptualization, there are two large categories of skills that make the use of the digital ecosystem friendlier and safer: *fundamental* and *instrumental*.

The former promote the reflective, ethical, and creative use of technologies, having critical thinking in the use of the web as their training axis, thus building capacities that involve analyzing, inferring, solving problems, arguing, making decisions, communicating, creating and use that thought to show a participatory stance in relation to the various issues that represent a challenge with the use of the Internet:

- Privacy, identity, and digital footprint.
- Reliableness and relevance of information.

- Operation of algorithms and their impact on daily life.
- Communication in the online universe, interaction on social networks.
- Creation of digital content with efficient and empathetic language.
- Use of the internet to participate in problem solving.

The second category corresponds to instrumental digital skills, which are those that are linked to the management of tools to have the ability to respond to specific needs and propose practical use of the devices. Within this category the most frequent skills are:

- The generation and use of email.
- The use of worksheets and spreadsheets.
- Making digital presentations.
- Apps downloading and installation.

In short, fundamental digital skills put citizens in better conditions to understand reality. This digital literacy seeks to empower people in all areas of life, so that they achieve their personal, social, educational, and occupational goals and can actively participate in society. "This is a basic right in a digital world, which promotes the social inclusion of all nations."

From an educational point of view, there are fundamentals that can be grouped into three groups for the purpose of teaching and learning about technology and its use and they are: respect, educate and protect.

Respect

- Digital access: Digital citizenship begins with equal digital rights and access.

- Digital etiquette: Are the conduct standards or way of proceeding with electronic media.
- Digital law: It is essential that users understand how to properly use and share the digital property of others.

Educate

- Digital communication: Choosing the right tools for secure and effective information exchange.
- Digital literacy: This is about how to find, evaluate and quote digital materials.
- Digital commerce: It is related to the possibility of acquiring or selling digital goods or services through ICT, or even business associations through them.

Protect

- Digital Rights and Responsibilities: Citizens should understand their basic digital rights to privacy and freedom of expression.
- Digital security and safety: Digital citizens need to know how to protect their information.
- Digital health and well-being: An important aspect of living in a digital world is knowing when to disconnect throughout the prioritization of time and activities online and offline.

References

- Bauman, Z. (2015). *Liquid modernity*. Fund of Economic Culture.
- Digital Citizenship - Concept, values, risks, and benefits. (2022). Concept. https://concepto.de/ciudadania-digital/#ixzz8CZq3YLFo

- Delgado, P. (2020). *Are we digital citizens or not? The reality of connectivity in the pandemic.* Observatory / Institute for the Future of Education. https://observatorio.tec.mx/edu-news/ciudadania-digital-pandemia/

- Expansion. (2022). What is digital citizenship and what are its characteristics? Expansion. https://expansion.mx/tecnologia/2022/05/03/que-es-la-ciudadania-digital-y-cuales-son-sus-caracteristicas

- Prensky, M. (2010). Digital natives and immigrants. Obtained from: https://www.marcprensky.com/writing/Prensky-NATIVOS%20E%20INMIGRANTES%20DIGITALES%20(SEK).pdf
- Morduchowicz, Roxana. (2021). UNESCO - Digital competencies and skills. Retrieved from: https://unesdoc.unesco.org/ark:/48223/pf0000380113.locale=en

Promoting the benefits of Digital Governance

Naldy Patricia Rodríguez Lagunes

In recent years, various concepts such as governance, open government, digital government, open parliament, among others, have been included in the language of public administration. All of them, regardless of their specific subject, have the same purpose: to satisfy people's needs, responding to social problems and guarantee respect for human rights.

Governance is a form of government whose characteristic is that decision-making actions in education, health, environment, administration of justice, among others are the result of a communication process between authority and population. It is the change from the vertical and subordination relationship between the government and the governed, to a horizontal one and collaboration between both actors. Although the authority executes the policies, they derive from the dialogue and surveillance of civil society, that is, it is citizen empowerment.

We can think of governance as the genus (communication between population and government) and specific policies as the species, such as Open Government Advisory Councils (regulated by Transparency laws), open parliament (communication to propose and monitor the issuance of laws) and Citizen Comptrollers (surveillance of public works and services), instruments that involve governance.

"The governance model for public administration comprises a broader idea of democracy than any of the other contemporary approaches (Peters, 2004: 69)."

So, what is digital governance?

It is undeniable that social interactions are increasingly common in the digital world: online education, home office, meetings through electronic platforms, online shopping, interaction on social networks and more, so it is difficult to imagine the today's world without the use of smart devices whose function is to bring people together and satisfy their needs.

Digital governance allows the relationship between government and population to occur through Information and Communication Technologies (ICT). Thus, a digital citizen uses these tools to participate in decision-making. The benefits are many: access to public services, improvement in government processes, cost reduction, eliminating the need to travel, promoting transparency and accountability, and facilitating citizen participation. All branches of public administration can be subject to digital governance.

Let's go to the examples, a student enrolls in his school remotely, digitizing and sending his documents, without having to go to the educational institution. A patient can schedule and access a medical consultation through video calls. The parties in a trial receive electronic notifications and promote proceedings through the same means. The authorities make any type of procedure available to the population to access the services they offer. Citizens can file complaints, make reports, and pay rights and obligations. Anyone can consult or request public information through digital platforms.

According to the United Nations, 40% of the world's population does not have access to using a computer. So, the biggest problem we face is getting internet service to the population, especially marginalized and rural areas, making it free and ensuring that people have devices to use it, which forces the authorities to adopt measures to expand this tool and exploit its benefits. However, with joint work between the population and the government, digital governance will become one of the main tools to locate, propose solutions and resolve social problems, in addition to ensuring the exercise of human rights.

References

- Juan and Giraldo Palacio, María Elena (2017). Governance, accountability, and transparency in local governments. In Aguilera Hintel, Rina Marisa (Coordinator). Aguilera Hintelholher, Transparency, and governance in local governments in Mexico. Library. Page 50. Retrieved on September 18, 2023 in

  https://www.researchgate.net/profile/Maria-Giraldo-47/publication/348419802_Gobernanza_rendicion_de_cuentas_y_transparencia_en_los_gobiernos_locales/links/5ffe3e3745851553a03d5b87/Gobernanza-rendicion-de-cuentas-y-transparencia-en-los-gobiernos-locales. pdf

- García, M. (2021) *Transparency, Access to Information and Subnational Governance in Mexico.* Gedisa, Mexico.
- Peters , G. (2005) *Governance and public bureaucracy: new forms of democracy or new forms of control?,* El Colegio de México, AC, available online at the link https://www.redalyc.org/pdf/599 /59911177001.pdf .
- United Nations. (sf). *The role of electronic governance in reducing the digital divide* | United Nations. https://www.un.org/es/chronicle/article/el-papel-de-la-gobernanza-electronica-en-la-reduccion-de-la-brecha-digital

Descriptive examples of positive and negative online behaviors.

Yolidabey Alvarado de la Cruz

Online user behavior is the acts or actions of people within a website, chats, apps, and social networks. Given the constant use of information technologies, ethical rules must be observed in the digital environment to generate respectful interactions. Some examples of positive and negative online behaviors are highlighted below.

Positive behaviors:

- Respectful communication on the internet: The communication we carry out online with other people must be respectful, since our comments can have a positive or negative impact on their family, social or work environment.

- Responsibility and care in the content that is shared and promoted: The information we disseminate must be substantiated and verified before sharing it, because disseminating or replicating information on social networks without verifying its veracity can cause harm to other people or commit crimes.

- Respect for other people's privacy: It is important to take care of people's privacy, asking for their permission before uploading or tagging them in a photo or video. This action prevents someone from being exposed without their consent.
- Make responsible use of digital tools: It is essential to know the scope of digital tools, the benefits, but also the harm that can be caused if they are used improperly.
- Foster positive relationships: Digital tools allow us to relate to the community, so we must respect the diversity of opinions, avoiding issuing aggressive comments that could affect third parties.

Negative behaviors:

- Violation of privacy: The right to privacy is that every person has to separate aspects of their private life from public scrutiny; however, with the use of new technologies, all our movements such as financial transactions, communications, etc., generate data that is recorded on the Internet, which is why it is sometimes obtained, bought and sold without the consent of the owner, which constitutes a violation of privacy.
- Fake news: They are also known as “Fake News” and are false or misleading information that is created, presented, or disclosed to deliberately deceive the population and that can cause public harm.

- Cyberbullying with sexual intent: It consists of those preconceived actions that an adult carries out through the Internet to gain the trust of a minor and obtain his or her own sexual satisfaction through erotic or pornographic images that he or she obtains from the minor.

- Identity theft: Consists of impersonating another person on the Internet. It is done by accessing the user's account or creating a false profile with the personal information of the impersonated person.

References

- García Ricci, D. (2013). Constitutional Article 16. Right to privacy. Human Rights in the Constitution. Comments on Constitutional and Inter-American Jurisprudence, t. I, 1045–1079. Obtained from: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf

- Computer Security and Incident Response Team (CSIRT). (2021). Fake News, The dangers of misinformation. Obtained from: https://www.csirt.gob.cl/media/2021/05/FAKE-NEWS-los dangers-de-la-desinformacio%CC%81n-ok-.pdf

- Panizo Galence, V. (2011). Cyberbullying with sexual intent and child-grooming. Criminology Notebooks: Journal of Criminology and Forensic Sciences, Obtained from: https://dialnet.unirioja.es/descarga/articulo/3795512.pdf

- Veracruzana University (2016.). What to do when faced with identity theft. Obtained from: https://www.uv.mx/infosegura/general/trabajos_suplantacion/.

Tips to assess the quality of online information and avoid the spread of fake news.

Oscar Raul Puccinelli Parucci

The Broadcasting of false, incomplete, erroneous, distorted, or intrusive information is a phenomenon that dates back to ancient times, but which has exploded unusually within the framework of web 2.0, social networks, and social engineering carried out through them, big data and generative artificial intelligence.

The fakes news , in its restricted meaning, refers to false stories that appear to be news, spread on the Internet or other media knowingly of their falsehood, with the aim of influencing the population or certain sectors of it with the aim of ensuring that their recipients make them stop doing something (e.g., vote for someone or not vote), generating benefits for those who carry out this beam or for those who hire those services, which may be of a personal nature (e.g., the social cancellation of a person), economic (discredit a competing product) or political (e.g., winning an election).

In a broader sense, fakes news include those disseminated with ignorance of their falsehood and those created in a humorous context (where parody is used for entertainment purposes of the recipient), but we will focus on the first typology, as it is the most worrying in terms of protection of human rights and the democratic system and is currently powered by generative artificial intelligence, which by allowing the direct creation of images and sounds whose inauthenticity is practically undetectable, leads to the very worrying phenomenon of deepfakes .

The recent emergence of fakes news on a global scale, is explained by technological, epistemological, economic, emotional and political factors that favor its

Broadcasting, especially on social networks, from messages directed at influential people chosen through social engineering techniques - which include profiling - to who are offered information in accordance with their convictions through "social cascades" (when what is said or done by influential people is followed) and "group polarization" (when groups come together to defend a more extremist version than the one they held).

This pressing problem has deserved responses from both the public sector (States and the international community) and the private sector (civil society, associations, information society service providers), aimed at detecting false information and operating on them and their creators and disseminators. Of course, this task is not simple, since determining whether news is false depends on what is considered true at a given time and place and leads to considering various factors – e.g., the social consensus about something, which can vary from time to time. time, as has historically happened to the "flat earthers ", once the majority. Furthermore, as soon as it is determined that a story is false, various fundamental rights of the people affected by the transmission of news come into conflict, on the one hand, and, on the other, the freedom of expression of its broadcasters, which is a preferred freedom that protects even false or erroneous speech. This requires carrying out a careful "weighing of rights", which requires attention to the subprinciples of adequacy, necessity, and proportionality.

State responses to fake news focus on detecting them and administratively or criminally sanctioning their authors or disseminators, and aim to raise awareness among the population, trying to protect people's "digital identity" and tend to the formation of a strong "digital citizenship" that empowers the members of society.

In this direction, the international community has adopted several documents (especially motivated by the impact of the Facebook-Cambridge Analytica scandal within the framework of the Brexit plebiscite and the election of Donald Trump in 2016), among which the issued annually since 2017 jointly by the special rapporteurs for Freedom of Expression of the UN and the OAS.

Regarding private responses, the media and large platforms mostly created specific tools in their services, websites, blogs, extensions for browsers and applications, warning labels, content removal, account suspensions or deletions, etc. For its part, civil society offers free services, mainly on the Internet, where the quality of content that may have a social impact is checked and its possible falsehood is warned.

Among the different types of reactions are the following: a) content identification responses; b) legal and policy responses regarding information producers and distributors, including legislative, pre-legislative and policy responses; c) national and international "counter-disinformation" campaigns, based on the construction of counter-narratives; d) responses specifically aimed at a specific problem, such as those related to elections, and e) responses within the production and distribution processes of information society services, specifically curatorial ones (mainly editorial and content policies that are reflected in the so-called community standards); the techniques and algorithms implemented by content publishing platforms, search engines and other related third parties (for example, browser add-ons), which may include experimental research methods with Artificial Intelligence to detect and limit the spread of disinformation, or provide additional context or information about individual articles and posts); those of demonetization and disincentives, which eliminate the profits of sites that violate publication policies, and those of support for victims of disinformation, through ethical, regulatory and educational responses, including guidelines, recommendations, resolutions, media literacy and content credibility data and labeling.

In this direction, these types of actors adopted the following types of measures: a) awareness-raising actions: through policies even shared with other actors, education campaigns, digital and media literacy, etc., all aimed at building a positive ecosystem against disinformation, empowering those who decide to combat it and providing effective strategies against the phenomenon; b) changes to the platforms' code, including algorithms, through recommendations; c) policy changes and moderation actions, both internally and externally for the elimination of content reported as illegal or contrary to community guidelines, and d) transparency and public relations actions, which provide information on the operation of the platform and how to face the challenge of misinformation

Finally, regarding advice for citizens on how to detect fake news, it should be kept in mind that false information can materialize whenever the following content is observed:

a) Satirical or parodic content (publication made with the potential to be misleading, even if the publication is not intended to cause harm).

b) Fake connections (titles, images and quotes that are unfaithful to the content).

c) Misleading content (distorted information to create a different reality).

d) False contextualization (genuine information located in a factual or temporal context different from the real one).

e) Impostor content (genuine sources are impersonated).

f) Manipulated content (information or images manipulated to deceive); and

g) Fabricated content (false content, designed to deceive and cause harm).

Keeping in mind these different possibilities of manipulation, and in order to differentiate real news from what is not, it is advisable to pay attention to the following characteristics of the dubious publication:

I. Message and linguistics:

a) Factuality: Verified and unbiased information, use of last names for citation.

b) Evidence: Statistical data, based on research.

c) Message quality: Journalistic style, edited and corrected,

d) Lexical and syntactic: Frequent use of "today" or the past tense,

e) Current interest: Conflict, human interest, protagonist.

II. Sources and intentions:

a) Sources of content: Verified sources, quotes and/or attributions, heterogeneity of sources,

b) Pedigree: Site or organization known or not, reputation of the author,

c) Independence: Affiliation of the journalist to the organization.

III. Structure:

a) URL: Type of format chosen at registration,

b) "About us" section (about us): Clarity and verifiability of authors and editors, availability and format of the "Contact Us" section (contact us), type and professionalism of the emails and contact methods of the professional organization.

IV. Network:

a) Metadata: Metadata indicating authenticity.

In the same direction, it is suggested to pay special attention to the following keys to detect fake news:

a) Be careful with headlines: Fake news often has eye-catching headlines in all caps with exclamation points and often shocking and unprecedented information.

b) Always examine the URL: A fake web address or one that copies a real one can indicate fake news. Check the characters of the URL carefully because they are always small details.

c) Investigate the source of the news: Especially before sharing or spreading it. Some social networks such as Facebook or Google have enabled the Fact button Checking so that users can certify the veracity of the information.

d) Pay attention to formatting: Many fake news sites have misspellings or strange layouts.

e) Look closely at the photos and do an image search: Fake news often contains manipulated images or videos, even based on authentic photos taken out of context.

f) Check dates: Fake news can have a meaningless timeline or include altered dates.

g) Check the author's facts and sources to confirm they are accurate: If the identity of supposed experts is not mentioned, the news may be false.

h) Check other news: If no other news source reports the same story, it may be false.

i) Consider that the story may be a joke, especially when the source of the news is known for its parodies: If the details and tone suggest that it was written with humor, it is not a fake news.

j) Be critical: Some stories are false on purpose and for hidden or malicious purposes.

References

- AECOC Innovation hub (2022) *Facebook fights against fakes news* . Spanish Commercial Coding Association. https://www.aecoc.es/innovation-hub-noticias/facebook-lucha-contra-las-fake-news/ .
- Álvarez, R. and Del Campo, A. (2021), *Fake news on the Internet: actions and reactions of three platforms* , Center for Studies on Freedom of Expression and Access to Information of the University of Palermo. https://www.palermo.edu/Archivos_content/2021/cele/papers/Fake-news-on-the-Internet-2021.pdf.
- Botero, C. (2017). *The state regulation of so-called "fake news" from the perspective of the right to freedom of expression,* in "Freedom of expression: 30 years after

the Advisory Opinion on the mandatory membership of journalists.” http://www.oas.org/es/cidh/expresion/docs/publicaciones/OC5_ESP.PDF .

- Broadband Commission for Sustainable Development (2021), *Balance Act: Countering Digital Disinformation while respecting Freedom of Expression.* UNESCO. https://en.unesco.org/publications/balanceact .
- Center for Studies on Freedom of Expression and Access to Information of the University of Palermo (2021). *Are the lies of public officials unsustainable or do they have far-reaching effects? Study on the obligations of the State and its officials to prevent the proliferation of disinformation* . https://www.palermo.edu/Archivos_content/2021/cele/papers/Disinformation-and-public-officials.pdf).
- European Commission (2018) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Tackling *online disinformation: a European approach”* , COM/2018/236 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236).
- European Commission (2018) Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Report *on the implementation of the Communication Tackling online disinformation: a European approach”* ; COM/2018/794 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0794.
- Commission European (2022), *The Strenghtened Code of Practice on Disinformation 2022* . https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

- Cortés, C. and Izasa , LF *The New Normal? Disinformation and Content Control on Social Media during COVID-19".* Center for Studies on Freedom of Expression and Access to Information of the University of Palermo. https://www.palermo.edu/Archivos_content/2021/cele/papers/Disinformation-and-Content-Control.pdf .
- Khan , I. (2021). *Report of the Office of the Special Rapporteur for the promotion and protection of the right to freedom of opinion and expression " Disinformation and freedom of opinion and expression "* . A/HRC/47/25. https://undocs.org/en/A/HRC/47/25 .
- Melo, V. (2022). *Fake News.* The Law, Buenos Aires.
- Molina, MD et al (2021). *Fake News Is Not Simply False Information: A Conceptual Explanation and Taxonomy of Online Content.* American Behavioral Scientist, 2021, vol. 65(2) 180–212. https://doi.org/10.1177/0002764219878224https://journals.sagepub.com/doi/full/10.1177/0002764219878224
- United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others (2017). *Joint Declaration on Freedom of Expression and Fake News, Disinformation and Propaganda* and *Standards on Disinformation and Propaganda.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- United Nations (UN) Special Rapporteur on Freedom of Opinion and *Expression and others (2018). Joint declaration on media independence and diversity in the digital age.*

https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.

- United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others (2019). *Twentieth Anniversary of the Joint Declaration: Challenges to Freedom of Expression in the Next Decade.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others (2020). *Joint declaration on freedom of expression and elections in the digital age* . https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others (2021) *Joint statement on politicians and public officials and freedom of expression.* https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression and others (2022) *Joint declaration on freedom of expression and gender justice* . https://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.
- Santos- D'Amorim, K. and Fernandes , MK (2021) *Misinformation, disinformation, and malinformation : clarifying the definitions and examples in disinfodemic times* . Electronic journal of library science and information

science , vol. 26, e76900. https://www.redalyc.org/journal/147/14768130011/html.

- Wardle , C. and Derakhshan , H. (2017) *Information Disorder: Towards an Interdisciplinary Framework for Research and Policy Making.* Council of Europe: https://www.europapress.es/sociedad/noticia-informe-encargado-consejo-europa-alerta-amenazarepresenta-desinformacion-mundo-20171031174624.html .

Technological discrimination in a digital citizenship world: a logical contradiction in the information and knowledge society

Massimiliano Solazzi

Digital citizenship (or cyber citizenship) is a concept that refers to a world in constant change, a field of new rights in a digital environment characterized by the hegemonic role of Information and Communication Technologies (ICT), which is being developed in a contextual framework of the Information and Knowledge Society (SIC). This dynamic context of globalization offers us generational, technological, and sociological changes, with growing interdependence and communication between different countries around the world, a new citizenship that is part of a more open and interconnected society, where the polysemic concept is highlighted, as well as the crucial and prominent role of information being the raw material to generate knowledge.

In this scenario, ICT has emerged to remain in the daily life of each person, a digital culture that develops in an accelerated change in individual and social habits, at work, in study and research, even in consumption, but also in the way of communicating and, therefore, in interpersonal relationships. To talk about digital citizenship is to talk about technology and a public space like the Internet, in which a set of rights and responsibilities are generated that belong to all of us, but also to the set of behavioral norms related to technology, a complex study that covers social, political, and cultural areas.

Between the eighties and nineties of the last century, throughout the world we witnessed unprecedented changes to the global structure of societies, a stage in history defined as the digital era, characterized by the digital revolution, with many new opportunities, but also with many challenges, a period that extends to the present day and that does not allow us to glimpse its end. The inclusion of ICT brings with it a paradigmatic change, with implicit challenges and impacts in the social sphere, for example, in access to information, now with unlimited sources, generating and forging learning environments and new knowledge, thus improving communication, due to its ability to reduce any geographical distance. A digital communication defined without barriers, with digital information considered a fundamental input to improve the quality of life, promote social management, citizen participation, as well as influence the economic activity and development of any community.

A new administrative worldview that is reflected in the new models of governance and public management, as well as the improvement of bureaucratic procedures and the quality of services, favoring the process of evolution of the Public Administration (PA), for example, to through electronic government (in English, *e-government)*, which has the specific purpose of improving the interaction between citizens and the State.

From all the above, a question spontaneously arises: Does anyone have the right to access technology? From an objective or normative point of view we could find an answer in article 6 of the Political Constitution of the United States of Mexico (CPEUM), where it is established that "The State will guarantee the right of access to information and communication technologies (...)" Therefore, anyone has the right to be a digital citizen and, therefore, to the use of technologies and the Internet.

Unfortunately, in the 21st century, we are witnessing the phenomenon of the Digital Divide (BD) (in English, *digital divide)* and technological discrimination, a new expression of the social stratification of the 21st century and an insurmountable limit for the exercise of the Right of Access to Information (DAI). By its definition, BD is "the social distance that separates those who have access to ICT from those who do not have it" (Cortés, 2009). In this regard, we can understand that with BD, the fragmentation of inequalities with respect to the distribution of wealth and its direct effect on the wage gap, as well as the existence of an imbalance caused by social fractures in the inequality of access and use of the internet, referring to factors such as education, language and content, in this sense, BD as a paradox and logical contradiction in the technological and knowledge society.

In conclusion, BD is an asymmetry grouped by different criteria and areas, a set of determining factors or variables among which the economic and educational level, geographical and cultural aspects, gender, and age, among others, stand out. From the above, social stratification in the world of digital citizenship has therefore a "digital stratification", we must remember that ICT demands more qualified human capital, adequate technical knowledge, accessibility to technological infrastructures such as, for example, devices electronics and Internet access.

References

- Ávila, D. (2014) *The use of ICTs in the environment of the new Mexican public management.* Mexico: Scaffolding vol.11 no.24. Recovered from http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-00632014000100014

- National Human Rights Commission (2015). Right to access and use of Information and Communication Technologies. Mexico: National Institute of Historical Studies of the Revolutions of Mexico. Recovered from https://appweb.cndh.org.mx/biblioteca/archivos/pdfs/foll_DerAccesoUsoTIC.pdf

- Political Constitution of the United Mexican States, published in the Official Gazette of the Federation on February 5, 1917, last reform published on June 6, 2023. Recovered from https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

- Cortés, J. (2009), *Review of "What is the digital divide?: an introduction to the new face of inequality."* Mexico: Library Research, UNAM. Retrieved from https://www.redalyc.org/pdf/590/59013270011.pdf

- Martínez, P. and Mesa, A. (s/f). *Electronic government and digital citizenship: a gap between policies and opportunities.* Spain: Spanish Association of Political Science and Administration. Retrieved from https://aecpa.es/files/view/pdf/congress-papers/11-0/900/

- Olarte, S. (2017), *Digital divide, poverty and social exclusion.* Spain: Labor Issues No. 138/2017. Recovered from https://dialnet.unirioja.es/descarga/articulo/6552396.pdf

- Solazzi, M. (2023). *The new expression of social stratification of the 21st century: digital divide and technological discrimination, a paradox of the information and knowledge society.* México: Encrucijada Electronic Journal of the Center for Studies in Public Administration, (45), 45–67. Recovered from https://revistas.unam.mx/index.php/encrucijada/article/view/86151

Digital citizenship and data protection from an academic perspective.

Maria de Leon Sigg

Technological innovations have given us the opportunity, and sometimes have also forced us, to live, learn and work digitally (Baltazar-Vilchis, Sámano-Ángeles, Martínez-Garduño, & Garduño-Martínez, 2020). In this sense, we have become digital citizens. This digital citizenship is exercised in different elements: access, commerce, communication, literacy, etiquette, law, rights and responsibilities, health and well-being, as well as security and integrity (Capuno, et al., 2022), and membership in it should be governed by principles analogous to those found in traditional citizenship, including respect, kindness, responsibility, and positive contribution to society (Ôztûrk , 2021).

In addition, a set of fundamental skills is required to function successfully in the digital world. These include the ability to find information online, detect suspicious content, pay attention to privacy policies with information collected online, and profitably use technology to participate responsibly with others (Hui & Campbell, 2018).

However, the diversity of profiles and interests of digital citizens, the variety of information uses and technologies, their accessibility, and the different legislation at the local, national, and international level, among other factors, complicate the exercise of rights. digital and the development of sufficient skills to actively participate in the digital environment. As a result, it is necessary to rethink the regulation of participation in digital societies, as well as the approaches and objectives of the education of the citizens who are part of them (Pangrazio & Sefton - Green, 2021).

Therefore, there are several tasks that the academy must address to promote the construction of good digital citizenship that encompasses the appropriate use of information and communication technologies, and, therefore, the protection of data. These tasks include ensuring adequate instruction on digital citizenship issues, generating new knowledge about the elements of digital citizenship, and linking the academy with all agents involved in this topic. To ensure training on digital citizenship issues, the academy must collaborate in the identification of audiences and their specific needs, define relevant content to understand and apply digital rights and responsibilities, develop innovative methods to develop digital skills and promote the values necessary to be exemplary digital citizens.

Likewise, it is still pending to analyze the integration of the concepts of digital citizenship in the training of children and youth in formal education, as well as in non-formal education for adult literacy in these topics. Furthermore, it is essential to consider the training of trainers and instructors with a strong ethical sense.

Regarding the generation of knowledge, the academy's task is to contribute to the development of technologies that improve the protection and access to data, identifying biases that may affect digital rights. Finally, academia must constantly collaborate with industry, government, other educational institutions and with autonomous bodies that work on the regulation of digital life.

References

- Baltazar-Vilchis, CA, Sámano-Ángeles, A., Martínez-Garduño, Y., & Garduño-Martínez, A. (2020). Analysis of digital citizenship in students of a university institution in times of pandemic. *In Crescendo, 11* (4), 425-441.
- Capuno, R., Suson , R., Suladay , D., Arnaiz , V., Villarin , I., & Jongoy , E. (2022). Digital citizenship in education and its implication. *World Journal on Educational Technology: Current Issues, 14* (2), 426-437.
- Hui, B., & Campbell, R. (2018). Discrepancy between Learning and Practicing Digital Citizenship. *Journal of Academics Ethics, 16,* 117–131.
- Ôztûrk, G. (2021). Digital citizenship and its teaching: A literature review. *Journal of Education Technology and Online Learning, 4* (1), 31-45.
- Pangrazio, L., & Sefton-Green, J. (2021). Digital rights, digital citizenship and digital literacy: What's the difference? *Journal of new approaches in educational research, 10* (1), 15-27.

III. ETHICAL BEHAVIOR IN DIGITAL ENVIRONMENTS

Online Responsibility Context

Erik Alejandro Cancino Torres

Technology and the Internet as fundamental components of society in the first two decades of the 21st century transcend all areas and influence all individuals in the construction of digital citizenship, understood according to Mossberger, Tolbert and

McNeal (2007) . as "the ability to participate in online society" (p.1). However, that is not the only and most important meaning that we can give to this social condition typical of those who have a high degree of digital literacy.

In this regard, UNESCO (2020) states that "digital citizenship involves a set of competencies that allows people to access, understand, analyze and use the digital environment, in a critical, ethical and creative way" (p.9). Therefore, it is appropriate to highlight that otherwise, those who do not have these skills are called digital immigrants, that is, those people born between 1946 - 1960 and 1960 - 1980, and who are part of the generational segments called *baby boomers* and generation X, respectively; for their part, those who were born immersed in a digitalized environment and see themselves as natural entities of this electronic context, are the individuals who make up generations Y, Z and Alpha, born between 1980 and 2023.

For this reason, it is essential that the members of society self-evaluate and determine according to their own demographic and psychographic characteristics in which case they identify themselves, since the recognition of their own abilities to practice will depend on this. their category of digital immigrants or digital citizens (natives). Without this implying a devaluation or inferiority due to belonging to one segment or another.

The relevance of achieving this self-recognition implies a great responsibility, aimed at the full exercise of the right of access to information, established in article 3 of the Federal Law of Transparency and Information Access, since everyone, without exception, in this country, regardless of our cognitive abilities in the technological context, we are empowered to exercise such an important prerogative.

Citizens or digital natives, through the effective use of electronic platforms that, in recent years, have been established to guarantee access to public information by citizens, as is the case of the National Transparency Platform, "a space in which you can consult everything produced or protected by public institutions in Mexico, and it is also the means to request information from them" (National Transparency System, 2023).

In the case of, digital immigrants (*baby boomers* and generation X) throughout the urge of a major self-digital literacy, so the technological breach between this generations won't be an ordinary impediment to the exercise of the right of information access of this broad population segment in Mexico and going on worldwide.

In this sense, the care and protection of the personal data of those of us who surf the Internet, both digital citizens and digital immigrants, also stands out for its importance, in such a vulnerable context, in which the high specialization of individuals in applied computer knowledge dishonest activities confront us with risks that we must overcome with skill and responsibility, so that the digital footprint that we leave in each of the actions we carry out on the web is not used in illegal practices.

The ability to navigate through the internet without being violated will always be our greatest purpose, as long as we remember that the privacy policy of our social networks, the advertising or privacy of our profiles, the authorization of the use of our personal data and the protection of our passwords or access codes, will at all times be constituted as the best tools in our favor so that the full exercise of our digital rights is materialized with the greatest legality, certainty and certainty.

References

- Mossberger, K; Tolbert, C, & McNeal, R. (2007). *Digital citizenship: internet, society and participation.* Cambridge: Mit Press.
- United Nations Educational, Scientific and Cultural Organization (2020). *Digital Citizenship. Curriculum for teacher training.* Montevideo: UNESCO.
- National Transparency System (2023). National Transparency Platform. Mexico: SNT.

Which are the ethical principles that should rule enacting in digital environments?

Javier Brown César

I am going to begin my reflections by talking about two crucial topics: citizenship and ethics. The idea of citizenship was born, like democracy, in Attica, specifically in Athens in the 6th century BC, thanks to the reforms of Solon and Cleisthenes.

It is vitally important to highlight that the birth of democratic institutions was due to laws (nomos). The laws are of such importance that those who created or reformed them were considered almost divine beings. In the case of Solon, he was one of the Seven Sages. Thanks to the laws, the Greeks emerged from the barbaric regime and created democracy.

Many of the main institutions of Athenian democracy survive and sustain contemporary democratic systems. Among these institutions we find:

The equality of all before the law (isonomy).

The freedom to speak in public spaces without restrictions (isegory).

Pay accounts.

And as the main result, freedom (eleutheria).

Democracy and freedom, since the Athenians, are an indissoluble binomial, which remains to this day.

I want to highlight the importance that the Athenians gave to accountability. Any unaccountable magistrate was subject to the highest possible penalty, after the death penalty, in Attic law: the trial of loss of citizen rights (atimia). This trial involved exile and confiscation of the assets of those who were not held accountable.

A fundamental institution linked to democracy and vital to its development and prosperity is citizenship. Aristotle defined citizenship as the ability to participate in public office. It must be remembered that, at that time, the government through magistracies was chosen by lot, in an Athens with no more than 40 thousand citizens. Furthermore, the original citizenship was exclusive: only for men, Athenians, with a minimum patrimony to have a *hople* (basic armor of the hoplite soldier).

Ethics was also born in Athens, thanks to the new ideas of Socrates. Before Socrates there were already deliberations on human actions, but all linked to natural elements or principles. The ethics that Aristotle systematizes consists, in summary, of a happy life thanks to the practice of intellectual virtues.

After this introduction, I am going to refer to the challenge of citizenship and ethics in digital environments.

I have started with the Greeks, because what they created is at risk in the digital world. I will update my reflections to the millennium we live in. Today we are in what the sub-Korean philosopher calls “The Swarm,” an expressive metaphor that reflects the informational situation that we suffer. In the swarm everyone moves feverishly without a clear end or fixed orientation. They all work for an absent or rather virtual queen.

The swarm creates the nightmare of Jorge Luis Borges's total library, the famous Library of Babel, with its incessant proliferation of information that generates astonishment and uncertainty. We are facing a global phenomenon that leads people to a kind of labyrinth in which we do not have Ariadne's thread, that is, we have no way out.

This informational chaos, I quote Byung-Chul Han: “The partner gives way to the solo. What characterizes the current social constitution is not the multitude, but rather loneliness... That constitution is immersed in a general decline of the common and the communal. Solidarity disappears. Privatization is imposed even in the soul. The erosion of community makes common action less and less likely” (p31-32). And this erodes democracy at its foundations, which today, according to Chul Han, becomes infocracy and the infodemic arises: “The attempt to combat the infodemic with the truth is... doomed to failure. It is resistant to the truth” (p 42). Furthermore: “Digital knowledge makes discourse superfluous” (p. 61).

I am going to leave the quotes here to focus on the challenges of ethics in the face of irreversible digitalization.

First, inequality, digital, like social systems, creates and deepens inequalities. The digital divide is not closing but widening and this forces a process of collective enlightenment in which there can only be participants, because authoritarian dirigisme annihilates free thought.

Secondly, superficiality. The digital world deprives us of the background, it is aesthetic, but not logical. It creates appearances but does not allow the truth to emerge or hides it, and this is where institutions that reveal the hidden, such as the INAI, are vital and indispensable, because they reveal the truths of government arcana.

Third, the empire of lies. We no longer talk about post-truth.

Fourth, ethics. Today ethics has been confined to specialized codes, to mere deontology. It has thus lost its original, Greek root. *Ethos* for the Greeks was more than behaviors, it is the abode from which good and noble, virtuous, in short, acts are born.

We must recover individual ethics and the imperative of the constitution of the subject. We must return to the imperative of turning life into a work of art, despite and even against a digital world that trivializes art, deconstructs the subject and leads us to what today is called posthumanism.

The idea of the human being and mainly the idea of the enlightened human being that Kant phrased as leaving one's minority and learning to know for oneself, is in crisis. Hence the cruciality of recovering the dynamics of subjectivation, that is, of the constitution of the ethical subject that takes its life to maximum fulfillment. Key in this sense is to guarantee the right to identity. In democratic systems this entails maximum transparency in the actions of the State, its subjection to citizen controls and its subordination to the power of the citizens; and, on the other hand, the jealous protection of personal data from any possible attack or reckless disclosure.

This entails recovering the capacity of language to constitute a public space today degraded as in Orwell's 1984. I end with a quote from Byung-Chul Han and a subsequent reflection: “Vocabulary is radically reduced, and linguistic nuances are eliminated to prevent differentiated thinking. Individuals are deprived of the ability to reflect in thought a reality, a world, other than that of the party” (p. 80).

The human being inhabits language, and the emptying of language is an emptying of the self. We must recover the word in the public space, fight against the empire of falsehood, and recover democracy from the revelation of power. We return to the Greeks and constitutive elements of the original democracy: the rule of law and that it is equal for all, the freedom to speak in the public space and the subjection of those who govern to a regime of accountability that It subordinates and ties them to a citizenry that must emerge from indifference to return to participation.

The Athenians called polities those who were citizens and interested in public affairs; on the other side were the idiots: citizens alienated from public space. It was the proliferation of idiots that, along with other factors, led to the collapse of democracy; It is the emergence of subjects who have returned to the original ethical imperatives of constituting their own life as a work of art and who are activated, informed and participate, the basis for our democracies to be sustainable.

What is artificial intelligence?

Norma Julieta del Río Venegas

It is a set of software, logic, computer science and philosophy disciplines that are intended to perform functions that were thought to be exclusively human, such as perceiving meaning in written or spoken language, learning, recognizing facial expressions; all this with the purpose of solving problems under given conditions, contrasting information, and carrying out logical tasks.

According to the Ibero-American Data Protection Network (RIPD), artificial intelligence (AI) is an "umbrella" concept, as it includes a variety of computational techniques and processes focused on improving the capacity of machines to perform different activities, which range from algorithmic models, through "machine learning" systems. (Fontanilla , 2020)

Types of artificial intelligence (INAI, 2022).

Reactive machines: These are the most basic type of AI; which are incapable of evolving and are based on decisions about the present (they have no memory).

Limited memory: Unlike reactive machines, they learn from the past using their own or transmitted previous experiences and behavioral rules and scenario information stored in their memory for decision making.

Self-awareness: It is still a hypothetical idea, but it constitutes the final phase of AI types. Its objective is the creation of self-aware machines with the ability to build a representation of themselves, their environment, and their own behavior.

Theory of mind: Presents systems or machines whose AI allows them to understand how their environment works, that is, the people, objects and other systems that surround them. In addition to providing means to interpret the expression of thoughts, emotions, and ideas, as well as to evaluate reasoning and behavioral processes.

The INAI developed specific recommendations for the processing of personal data derived from the use of artificial intelligence, which highlight the risks and proactive responsibility in the design of information technologies with a focus on this type of intelligence, which will allow, create effective control practices, procedures and tools for the management and care of the personal data of users who make or make use of said technologies. (INAI, 2022)

These recommendations cover those technologies that handle large amounts of information and personal data to operate, since these are essentially the ones that require guaranteeing the security of the information with compliance with the regulations on the matter. In Mexico, various initiatives are being discussed regarding cybersecurity and the regulation of artificial intelligence. Recently the Chamber of Representatives received the initiative for the creation of the Law for the ethical regulation of artificial intelligence, which proposes developing a legal framework for Mexico that regulates the ethical use of artificial intelligence and robotics.

The proposal seeks to create the Mexican Council of Ethics for Artificial Intelligence and Robotics (CMETIAR), made up of representatives of the government, human rights organizations, Congress, and private sector agents.

The INAI is protected through comprehensive solutions (software and hardware), with an architectural deployment of layered security that allows the traffic that travels through the Internet links, both inbound and outbound, to be kept available and secure using new generation devices for access control, protection from intrusions and new generation attacks. The institute has a perimeter security system, which serves to contain attempted attacks that are directed at its internal systems.

References

- Frontanilla, MC (June 11, 2020). Codas Studio. Obtained from http://www.estudiocodas.com/2020/06/11/la-inteligencia-artificial-y-el-derecho/

- INAI. (May 1, 2022). *INAI digital library*. Obtained from https://home.inai.org.mx/wpcontent/documentos/DocumentosSectorPublico/RecommendationsPDP-IA.pdf

Ethical behavior in the use of artificial intelligence

Carlos Languendik Muñoz

Artificial intelligence (AI) is experiencing rapid development and extraordinary progress in recent years, surpassing human performance in complex tasks such as image recognition and strategic games. However, the growing integration and implementation of AI in different areas such as health, justice and finance entail significant ethical risks (Mittelstadt et al., 2016) that must be addressed.

Algorithmic biases, lack of transparency and threats to privacy are the main ethical challenges in the use of AI; The first of these addresses the possibility of amplifying human biases, because algorithms learn from data that reflect stereotypes and social prejudices (Cath , 2018). This can lead to algorithmic discrimination to the detriment of certain groups.

Another key challenge is the lack of transparency in AI systems, which makes it difficult to evaluate their ethical and social impacts. Also, the use of AI presents threats to privacy, due to the large amount of personal data used by these systems. Finally, AI can have unintended negative consequences by automating decisions in complex areas such as healthcare and criminal justice.

This is why ethical approaches must be explored in order to promote ethical behavior in the development and use of AI, given that it is crucial for it to fulfill its potential as a tool that benefits society; therefore, a central idea is human-centered design, since it puts the well-being of people first in all stages of the life cycle of AI systems (The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems , 2019).

Likewise, participatory algorithmic governance advocates the inclusion of multiple actors in the evaluation of AI technologies, such as experts, users, and potentially affected groups (Katzenbach, Ulbricht , 2019) . These approaches seek to ensure that AI respects human dignity and rights.

Based on this analysis, several recommendations are proposed to promote ethical behavior in the use of AI:

- To audit algorithms for biases detection, evaluate their impacts and increase transparency.
- Encourage diverse and inclusive AI development teams.
- To adopt specific regulations for AI in areas of high ethical impact.
- Integrate ethical considerations into all stages of AI design and deployment.
- Improve education on AI ethical principles among developers and users.
- Promote citizen participation in AI governance.
- Prioritize the privacy and autonomy of individuals.

Conclusion

AI presents profound ethical challenges that must be addressed so that this technology is developed in a way that is aligned with human values. The adoption of ethical approaches, appropriate regulations and best practices by multiple actors can promote ethical use of AI that maximizes its benefits to society. Ethical behavior is the key to AI delivering on its promise to improve human life.

References

- Cath, C. (2018). Governing Artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A,* https://doi.org/10.1098/rsta.2018.0080
- IEEE Advancing Technology for Humanity (2019) "Ethical Aspects of Autonomous and Intelligent Systems" https://globalpolicy.ieee.org/wp-content/uploads/2019/06/IEEE19002.pdf
- Katzenbach, C., Ulbricht, L. (2019) "Algorithmic governance", *Internet Policy Review* , https://policyreview.info/concepts/algorithmic-governance
- Mittelstadt, B., Allo , P., Taddeo, M., Wachter , S., & Floridi , L. (2016). The Ethics of Algorithms: Mapping the debate. *Big Data & Society,* https://doi.org/10.1177/2053951716679679

Explanation of the importance of developing media and digital education skills

Naldy Patricia Rodríguez Lagunes

Until 2022, it is estimated that there are 93.1 million Internet users in Mexico, which generally represents 78.6% of the population aged six years or older. Data that represents an increase of 3.0 percentage points compared to 2021.

These statistics are modified and reduced according to the territory. In the urban area, 83.8% of the population aged 6 or older used the Internet, while, in the rural area, 62.3% of the population used this tool, according to the National Survey on Availability and Use of Information Technologies in the INEGI households of 2022. That is, there is still a digital divide that remains in the country between an urban and a rural region.

The disparity is also observed in the conformation of the territory: the states that observed the highest values in the proportion of internet users were Baja California and Mexico City with 89%; while the states that recorded the lowest values were: Guerrero (67.5%), Oaxaca (62.5%) and Chiapas (56.7%).

Social conditions increase the inequality breach. During the international pandemic generated by COVID-19, it is estimated that 26 million students under 16 years of age in the country stopped attending school for a year and a half when they did not attend classrooms in person. A greater number of families had difficulties following up on school activities, which reduced learning for Mexican children.

In 2022, the age group that concentrated the highest percentage of internet users was 18 to 24 years old, with a participation of 95.1 percent. The groups of 25 to 34 years old and 12 to 17 years old followed, with 92.8 and 92.4%, respectively.

In fourth place was the group of users aged 35 to 44 years, who registered 87.1%, while the group of people who used the Internet the least was those aged 55 or older, with a participation of 47.6%.

Two more indicators must be analyzed: The use that people give to the internet and what devices they connect from.

The three main means for connecting users to the internet: smart cell phone with 96%, laptop with 33.7% and a television with internet access 22.2%.

While the main activities carried out by internet users are to communicate (93.8%), access social networks (90.6%) and entertainment (89.6%). Making payments via internet increased from 18.3%, in 2019, to 26.9%, in 2022. In contrast to the above, reading newspapers, magazines or books decreased from 47.1 to 39.9%, in the same period.

To the shortage of internet and technological equipment in rural areas of Mexico, we must add the lack of media literacy of those who are mothers, fathers, or legal guardians, who in general have less use of digital platforms.

As the Inter-American Court of Human Rights warns in the Case of Gomes Lund and other v Brazil (2010) "in a democratic society it is essential that state authorities be governed by the principle of maximum disclosure, which establishes the presumption that all information is accessible."

States have, as part of their general obligations, a positive duty of guarantee with respect to individuals subject to their jurisdiction. This means taking all necessary measures to remove any obstacles that may exist so that individuals can enjoy the rights that the American Convention on Human Rights recognizes. (Cantos vs. Argentina Case, 2002)

Mexico and its families live in such different realities and asymmetrical conditions that it is necessary to follow through differentiated actions in each region and geographical area to provide the ideal tools to the entire population so that they can use information technologies correctly and efficiently and communication.

As statistics indicate, digital literacy efforts should focus on adults who are in the process of adapting to change. And in the case of childhood, rather than teaching how to use devices and tools, the proper use of platforms should be encouraged to mitigate important risks.

References

- Inter-American Court, Case of Cantos vs. Argentina, (Merits, Reparations and Costs), Judgment of November 28, 2002, Series C No. 7, para. 49. https://www.corteidh.or.cr/docs/casos/articulos/seriec_97_esp.pdf
- Inter-American Court, Case of Claude Reyes et al. Chile, (Merits, Reparations and Costs), Judgment of September 19, 2006, Series C No. 151, para. 92 https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf
- INEGI, National Survey on Availability and Use of Information Technologies in Homes of 2022. https://www.inegi.org.mx/programas/dutih/2022/

Explanation of the importance of developing media and digital education skills

Julio César Bonilla Gutiérrez

The contemporary era, characterized by its accelerated technological advancement, has drastically transformed the way we understand, consume, and disseminate information. The omnipresence of digital devices and the communications revolution have generated a vast sea of information. In this panorama, media and digital literacy skills emerge as fundamental for the 21st century citizen (Lee, 2019). Let's see why it is essential to delve into this topic.

1. Safe Browsing in the Digital Environment, Fake News, and promotion of critical thinking

With the Internet and smart devices, in almost every corner of the world, our exposure to digital information and interactions is constant. However, this unrestricted access also comes with many different risks.

Cyberbullying, for example, has emerged as a real threat in digital spaces, especially affecting women, young people and adolescents. People who are not familiar with digital etiquette and safety regulations can easily become victims of harassment or even become stalkers without realizing it (Johnson & Turner, 2020). Phishing, another growing problem, is an online fraud technique that tricks people into providing personal information, such as passwords or credit card numbers. Against these types of problems originating from the digital world, but with clear and proven consequences in the material world, adequate digital literacy teaches us to recognize and avoid these traps (Johnson & Turner, 2020). The information age has also been nicknamed, unfortunately, the age of misinformation. Fake news, or *fake news*, have become a propaganda and sometimes lucrative tool. These news stories are designed to appear credible, taking advantage of legitimate media formats and styles to mislead the reader.

Robust media literacy enables people to identify these news stories. It teaches us to verify sources, contrast information and recognize the signs of misleading content.

This ability not only prevents the spread of falsehoods, but also fosters a more informed and critical public (Smith, 2021).

Media and digital literacy go beyond simply understanding how media and digital tools work. It is about developing critical thinking about the information we consume. Not all content is neutral, and it is essential to recognize the agendas, biases, and intentions behind the information we access.

Critical analysis skills allow individuals to examine the validity, relevance, and reliability of information. This not only protects us from misinformation, but also encourages a deeper and more nuanced understanding of the issues (Lee, 2019).

2. *Active Participation in the Digital Society and Digital Education*

The digital world has brought with it new forms of civic, social, and political participation. From social movements organizing online to access to digital government services, being digitally literate means having a voice and power today.

For example, many political decisions and awareness campaigns now have a strong online presence. Those who understand how these media work can participate more actively, whether by sharing information, voting in online polls, or simply being more informed about current issues (González-Pérez & Hernández, 2022). Learning is no longer confined to classrooms. Online educational platforms, MOOCs (massive open online courses) and online tutorials have democratized access to education; those with digital skills have a variety of learning resources at their disposal, from courses from prestigious universities to practical skills taught by experts.

Digital education offers flexibility, allowing people to learn at their own pace and according to their own needs. However, it is crucial to have the skills to discern between quality educational sources and less reliable or misleading content (Martínez, 2020).

Conclusion

In an interconnected world, media and digital literacy skills are no longer optional, but essential. From protecting ourselves in the digital environment to actively participating in our society and taking advantage of educational opportunities, these skills equip us to be informed, critical and active citizens in the 21st century.

References

- González-Pérez, A., & Hernández, B. (2022). *Digital society: A new paradigm of learning and communication.* University of Barcelona Editions.
- Johnson, R., & Turner, L. (2020). *Digital Security: Protection in the Cyber Age.* Modern Editorial.
- Lee, J. (2019). *Skills for the digital age: Media literacy in the 21st century.* Oxford University Press.
- Martínez, L. (2020). *Online education: Opportunities and challenges of digital learning.* Educational Publishing.
- Smith, R. (2021). *Disinformation in the digital age: Identify and combat fakes news.* Cambridge Press.

Taking conscience about the importance of being responsible digital citizens at a global level

Julio César Bonilla Gutiérrez

Within the framework of the "Regional Conference on Municipal Transparency, Digital Citizenship and Accountability", fundamental issues related to digital transformation and its impact on today's society were addressed.

The importance of digital citizenship in the era of artificial intelligence was highlighted by highlighting its role in the construction of safe digital environments and in the promotion of social advantages that can be shared in their fruits, usefulness, and benefits.

In an interconnected world, it is essential to understand the crucial aspects of digital citizenship today, where the omnipresence of various artificial intelligences requires the construction of responsible digital citizenship. This citizenship involves the adoption of rights, responsibilities, and appropriate behaviors in the digital environment.

In this sense, some of the significant advantages of building responsible digital citizenship arise:

Access to Information and Education: Digital citizenship facilitates access to online information, promoting education, research, and continuous learning. Digital technologies allow access to specialized knowledge and enrich the ability to make informed decisions.

Global Communication and Collaboration: Digital technology enables instant communication and collaboration at a global level, breaking geographical barriers and promoting diversity and cooperation.

Educational and Employment Opportunities: Digital citizenship expands educational and employment opportunities by providing access to online educational programs and remote work opportunities.

Citizen Participation and Activism: Digital platforms allow activism and citizen participation, empowering people to express opinions and promote social and political causes.

Construction of Secure Digital Environments: it is of fundamental importance to guarantee secure digital environments. In this regard, some key aspects are:

A) Privacy and Personal Data Protection: Need for strong data protection regulations and transparent practices by companies to protect user privacy.

B) Cybersecurity and Cyberbullying Prevention: Responsible digital citizenship requires online security measures to prevent threats such as cyberbullying and identity theft. Public policies and awareness are essential in this area.

C) Digital Literacy and Critical Thinking: Promoting digital literacy and critical thinking is essential to evaluate online information and protect against manipulation and misinformation.

D) Digital Responsibility and Ethics: Fostering an ethical digital culture is essential to creating safe digital environments. Users must take responsibility for their actions online and respect the rights of others.

Responsible digital citizenship offers significant benefits and is essential for building safe digital environments. Privacy protection, cybersecurity, digital literacy, and online ethics are fundamental elements. Strong public policies, education and collaboration between diverse actors are crucial to achieving responsible digital citizenship and safe digital environments. Ultimately, digital technology can be a safe and beneficial space for everyone, boosting the development and well-being of society.

IV. DIGITAL RIGHTS

Fundamental rights of people in the digital environment

Joel A. Gómez Treviño

What most defines Web 2.0 is the explosion of user-generated content (a fundamental bottom-up process).

Since the emergence of Web 2.0, human coexistence has turned to the most popular social networks. According to the popular site "Statista", Facebook has 2,958 million monthly active users worldwide, YouTube 2,514 million, WhatsApp 2,000 million, Instagram 2,000 million, TikTok 1,051 million and Telegram 700 million.

According to the United Nations (UN), human rights must be respected both online and offline. Digital technologies provide new means to exercise human rights, but too often they are also used to violate them. Data and privacy protection, digital identity, the use of surveillance technologies and online violence and harassment are issues of particular concern.

The UN Secretary-General's roadmap for digital cooperation that ensures the protection of human rights has pointed out the way forward:

- ✓ Position human rights at the center of regulatory frameworks and legislation on digital technologies.

- ✓ Greater guidance on the application of human rights standards in the digital age.
- ✓ Address protection breaches created by evolving digital technologies.
- ✓ Discourage general internet shutdowns and generic blocking and filtering of services.
- ✓ National human rights-based laws and practices for data privacy protection.
- ✓ Clear and specific company actions to protect privacy rights and other human rights.
- ✓ Adopt and improve safeguards related to digital identity.
- ✓ Protect people from illegal or unnecessary surveillance.
- ✓ Laws and human rights-based approaches to address illegal and harmful online content.
- ✓ Ensure safe online spaces, transparent and responsible content governance frameworks that protect freedom of expression, avoid overly restrictive practices, and protect the most vulnerable.
- ✓ Guidance for the entire United Nations System on human rights, due diligence, and impact assessments in the use of new technologies.

The human rights that will be at greatest risk on the internet are the following:

1. Right to freedom of expression.
2. Right to equality and prohibition of discrimination.
3. Freedom of work or profession.
4. Freedom of the press.
5. Freedom of association, assembly, and demonstration.
6. Right to the inviolability of private communications.

7. Right to personal data protection.
8. Right to identity and free development of personality.
9. Right to work.
10. Rights of children and adolescents.

Since social networks represent spaces of a private nature, under the command and control of a single private entity, it is easy to limit or even nullify the rights of users. It will require hard joint work between social media officials, the information technology sector, academia, NGO's and the government, to analyze from a "multi-stakeholder" perspective what will be the best way to regulate or self-regulate digital spaces for social coexistence, always seeking respect for the human rights and digital rights of users.

References

- Biggest social media platforms 2023 | Statist. (2023, August 29). Statista. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
- Gómez, JA (2022). The Challenges of Human Rights in the Metaverse. In A. Delgadillo (Coord.), *Information Technologies* (1st ed., pp. 55 to 68). Editorial Human Rights Commission of the State of Mexico. Obtained from: https://www.codhem.org.mx/wpcontent/uploads/2023/01/Dialogos_DH_11_int_03_digital.pdf
- Tsekeris, C., & Katerelos, I. (2012). Web 2.0, complex networks, and social dynamics. Contemporary Social Science, 7, 233 – 246. https://doi.org/10.1080/21582041.2012.721896

Fundamental rights of people in the digital environment

Adrián Alcalá Mendez

In the recent "Regional Conference on Municipal Transparency, Digital Citizenship and Accountability" carried out by the National System of Transparency, Information Access and Personal Data Protection, in collaboration with the Commission for Entailment, Promotion, Broadcasting and Social Communication from the SNT, I had the honor of participating in the Central Region; Oaxaca, in the panel titled "Digital Citizenship, safe environments, privacy and personal data protection."

First, it is important to mention that, to understand the implications of Transparency, Digital Citizenship and Accountability, we must recognize that, over time, communication between people in electronic media has increased, hence, among daily activities, it is undeniable that the Government and society need to evolve and adapt to a new reality.

One of the most recent examples is the use of electronic platforms in education, during the health emergency caused by COVID-19, a strategy implemented by the Federal Government to provide continuity to basic education school cycles.

That is why the recognition of the right to the protection of personal data, by virtue of interactions in the digital environment and, especially, those related to public policies between the Government and citizens through electronic means, necessarily involve the processing of personal data.

In this context, it is important to highlight that, during the session held in October 2022, the Personal Data Protection Commission of the National Transparency System, approved the “Bill of Rights of the Individual in the Digital Environment”, which from a non-binding perspective, mentions the rights that a user of information and communications technologies has, the authorities that would protect you against any rights violation, as well as the way to maintain ownership and full availability of your personal data.

It also establishes the rights of universal access to the internet, identity, non-discrimination, privacy, protection of personal data and the use of social networks. It contains interesting innovations in the field, such as the right to digital inheritance, democracy, and good digital government. Among the most relevant ones stands out: the right to receive truthful information, such as the possibility of freely and without limitation monitoring the social networks of public servants, and digital rights versus the Public Administration, which guarantees every person access to public services and digital relations with public administrations.

At the INAI, we create tools that promote a culture of personal data protection for compliance with regulations on the matter. An example of this is the “Recommendations to keep your privacy and personal data safe in the digital environment”, a document that contains a series of practical tips on security settings, mobile applications, and software in general, useful for users to keep them safe your privacy and personal data in the digital environment.

Finally, it is important to mention that, with the increase in the use of new technologies, it is necessary to rethink the challenges that the protection of personal data entails, so expanding the regulatory framework to guarantee greater security for users is a priority.

Fundamental rights of people in the digital environment: free speech and privacy

Héctor Guzman Rodriguez

The enumeration of fundamental personal rights in the digital environment presupposes the acceptance of a generic concept related to the DIGITAL ENVIRONMENT.

It is proposed to resume the definition provided in the Regulations of the Federal Law of Personal Data Protection Held by Private Parties:

It is the area made up of the combination of hardware, software, networks, applications, services, or any other information society technology that allows the exchange or computerized or digitized processing of data.

The foregoing, without prejudice to carrying out a review or expansion in view of the interference and importance of artificial intelligence.

A second general budget is proposed, relative to the position of rights in the digital environment, compared to their corresponding rights in the physical environment, from which it must be established that, except for modulation or adaptation to the corresponding environment (digital or physical), no There are objective bases to define that there are better rights or rights of greater importance in one environment or another.

Proposal for enumeration of rights:

This illustrative list aims to establish the rights that, within the framework of digital law, must be regulated to define their characteristics:

Right to privacy: One of the most questioned rights in recent times, due to the erosion and intrusion that various technologies and digital platforms have had on this right; It is essential to state that the right to privacy in the digital environment does exist, but that it must be protected and built in consideration of the specific characteristics of that environment, precisely.

Right to privacy in work environments: In the face of the expansion of hybrid work models, it is necessary to regulate the balance that must exist between the employer's right to supervise employees and the right of employees not to be subject to disproportionate monitoring.

Right to the personal data protection: Expansion of its protection by updating the current legal framework, to address the progress made in the last 15-20 years in the field of technology.

Universal Internet access: Recognize and regulate that, facing the 2030s, it is not conceivable that the entire population of Mexico does not have access to a minimum level of service to access the Internet from home or, at least, from an existing public center in all towns in the country.

Right to digital education: Recognition of the right to obtain education to avoid "digital illiteracy" among the entire population and the obligation of the state to provide training to teachers in charge of the subjects that are designed to guarantee this right; obligation to provide public institutions with the necessary resources to guarantee this right.

Right to digital disconnection in work environments: It is necessary to regulate the way in which employers communicate or supervise employees outside of the working time that they have agreed to legally or conventionally, so that there is effective respect for their working time. rest, permits, vacations, as well as your personal and family privacy; it is necessary to prohibit dismissal for reasons related to the digital disconnection to which workers are entitled.

Right to protection of children on the Internet: Specific regulation for the protection of minors under 14 years of age in the digital environment.

Right to protection of adolescents on the internet: Specific regulation for the protection of those over 14 and under 18 years of age in the digital environment; recognition of "digital emancipation" for people between 14 and 17 years old, recognizing the emotional and intellectual maturity that allows them to make informed decisions in the digital environment, without the need for the direct and immediate participation of their parents and guardians.

Information and privacy in the face of video surveillance systems, with particular relevance in public systems: Whose objective must be to ensure the proportionality of the technology used to video monitor public and private spaces, as well as respect for the reasonable expectation of privacy in each case.

Right to be forgotten in Internet searches: Right for internet search engines to eliminate from the lists of results obtained after a search carried out based on their name the published links that contain information relating to that person when they are inappropriate, inaccurate , not relevant, not updated or excessive or have become such due to the passage of time, taking into account the purposes for which they were collected or processed, the time elapsed and the nature and public interest of the information.

Right to information: Equivalent to the same right existing in the physical environment.

Right to freedom of expression: Equivalent to the same right existing in the physical environment.

Right to digital will or transmission of digital last will: Possibility of going to digital service providers to access content of the deceased and give the instructions they deem appropriate regarding its use, destination, or deletion (recognized to the same people who would have equivalent rights in the physical environment).

It is proposed to define the powers of the Federation and the States in each case, to define whether the Congress of the Union (in the first instance) has the exclusive power to legislate on the digital rights of citizens.

Existing powers must be defined in favor of existing authorities and, where appropriate, the need to legislate on new powers and/or authorities in charge of the application of a possible Federal Law on Digital Rights.

Definition of a budget item for the protection and defense of citizens' digital rights.

References

- Official State Gazette (2018) *Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights.* Available in https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
- Government of Spain (2021) *Charter of Digital Rights.* Available at: https://www.lamoncloa.gob.es/presidente/activityes/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

People's responsibilities in the digital environment: respect and protecting online safety

Salvador Romero Espinosa

The digital environment is a public space in which people have responsibilities, since, although we find a universe of opportunities to exercise a series of rights, there is also many violations to which we are exposed at all times.

But what do we mean by responsibility? According to the Royal Spanish Academy, it is understood as the capacity existing in every active subject of law to recognize and accept the consequences of an act freely carried out.

Thus, to enjoy any right it is necessary that our rulers and institutions fulfill the responsibility of establishing all the necessary means to guarantee its exercise, as well as adequate education to easily access it, with all the implications and repercussions that this may have.

Likewise, they have the responsibility of demanding compliance with these guarantees from those involved and must be accountable to the governed regarding their actions to guarantee rights.

And that is where we all become co-responsible: citizens, adults, girls, boys and adolescents, the private sector, institutions, and, of course, the authorities, always keeping in mind that we must especially look after the rights of the most vulnerable people and sectors.

In that sense, all people have the right and responsibility to educate ourselves and educate us about and through the digital environment and the new rights and new social, economic, and cultural structures that its permanent use entails.

It should be noted that the rules of coexistence in digital environments, from origin, should be the same as those provided for in the legal and social norms of a community, however, with the passage of years and the increase in use of these environments, it is important that some rules are established focused particularly on coexistence on these platforms.

To this end, I would like to refer to some of what I consider should be recognized as the most basic responsibilities that we have as users of digital environments:

- Respect other users, without denigrating, ridiculing, or violating the ideas or rights of other people in any way when using digital media.
- Use appropriate language and appropriate behavior when interacting.

- Make responsible use of information.
- Use technology healthily so that it does not interfere with our physical and emotional well-being.
- Report any misuse of technology to the authorities.

By taking these measures we will be helping to have digital citizens who are committed, responsible and aware of their rights and obligations in the digital environment.

References

- Catalan charter for digital rights and responsibilities (2019). Generality of Catalonia. Available at: https://politiquesdigitals.gencat.cat/web/.content/00-arbre/ciutadania/drets-responsabilitats-digitals/versio-es/Carta_v2_ES_.pdf

Misinformation and cybersecurity

Anahiby Anyel Becerril Gil

In this era of digitalization [9]and datafication, everything is data (Simon, 2013), or will be. As individuals we have depersonalized and quantified ourselves, evolved into data; We are zeros and ones [10], dispersed in national and international databases, and it is through profiling and predictions made based on our information that defines and identifies us in the digital world. We have transformed

[9] Digitization, and the technology that made it possible, has made invasions of privacy more pervasive, widespread and prevalent, more frequent because we can obtain much more information about any person than before, more widespread because the technology for invasions is It is available to almost everyone and more prevalent because we are all a person of interest to someone who can now easily know something that was inaccessible before the digital age.

[10] Alluding to the binary system, made up of "1" and "0", which is used by computers to store information.

from atoms to bits. We have a legacy of data and information, of which our digital "ME" is made up.

Our personal data is not static, it is dynamic, it is under constant review and analysis, in addition to constituting the reusable resource of the digital market. They are information assets that do not depreciate, their richness and variety allow their multiple reuses, generating more value. For effective use, they must lead to action. The DIKW model (*Data, Information, Knowledge*, *Wisdom*) sets the standard for its use. In this way, once the data is collected, it must provide us with information, the information that allows us to obtain knowledge to finally generate wisdom that supports decision-making. The subjects of the data ecosystem [11]are in search of this wisdom, because, in the best of cases, it is the way to understand us and thus offer us services, develop applications, and send us "suggestions" for decision making. In other cases, this information allows the manipulation [12]of individuals for multiple purposes (malicious or not).

1. Digital citizenship

Digital citizenship not only gives us rights, but also attributes responsibilities in the digital environment. As digital citizens we are committed to acting ethically and safely in the digital environment. We need the development of skills and capabilities in cybersecurity, for which this must be constituted as an accessible and affordable right. It is our duty to get involved in the protection of our privacy and personal data, while responsibly using digital media and services. We also have co-

[11] The individuals or groups of individuals to whom the data concerns, those who collect the data, those legally responsible for the data, and various potential parties who may use it or wish to use it.

[12] An example of the concern about manipulative capacities in the social and political behavior of individuals is found in the declaration of the Committee of Ministers of the Council of Europe adopted on February 13, 2019. https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

responsibility in the co-creation of digital content, its consumption and access, as well as digital communication and discourse. For this reason, the construction of a decalogue of digital citizenship is proposed.

2. Cybersecurity to protect digital citizenship.

The Internet and the diversity of digital technologies that have been developed from it have given us new opportunities to develop endless tasks in the digital sphere. However, like any other technology, they have also been accompanied by various threats, which seem to be increasingly sophisticated.

There is no doubt that technology can influence the opinions and behavior of users. A variety of malicious actors have relied on this to manipulate and influence their decisions. Currently we live in an "information regime" (Han, 2022), in which its processing through algorithms and Artificial Intelligence (AI) tools decisively determines social, economic and political processes. The combination of automation, profiling, targeting or micro- targeting and marketing has had a significant impact on public opinion during (Becerril, 2021), fundamental stages in societies and democracies, in addition to facilitating control over people and mass surveillance, providing information that is not always true. AI fundamentally alters the way it is generated and spread by malicious actors. Automated networks of fake accounts can send messages more easily, at greater speed and scale, than real people. Thus, misinformation is one of the main threats that exists to undermine our digital citizenship. It constitutes a disruptive cybersecurity threat, were malicious actors hack humans instead of systems.

Therefore, the importance of developing capabilities to promote rational digital citizenship that combats misinformation. It is essential that digital citizens are informed and adopt good cybersecurity practices, such as:

- Education and awareness: Identify social engineering techniques and deception tactics such as bots, cyber-troops and cyborgs, as well as their false or malicious content.
- Verification of sources: Before sharing or acting on the information received. In addition to using reliable sources and contrasting information, providing verifiable and supported information, promoting transparency.
- Technology: Develop and use false or misleading content detection tools, such as content analysis systems and anti-spam filters; information verification labels that indicate whether it has been verified; security alerts for false or potentially malicious content.
- Collaboration: Collaboration between diverse actors can reduce the spread of misinformation.
- Promotion of critical thinking: As digital citizens we have the duty to question and critically analyze the information that circulates online; among others.

We as digital citizens are the first line of action. It is up to us to raise awareness about the risks and threats that exist in the digital environment, as well as the importance of keeping ourselves protected in it.

References

- Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes (2019). European Council. Available at:

https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

- Becerril, A. (2021). Challenges for the legal regulation of Artificial Intelligence in the field of Cybersecurity. IUS Magazine, pp. 9-34.
- Han, B.-C. (2022). Infocracy. Digitalization and the crisis of democracy. Mexico City: Taurus.
- Simon, P. (2013). Too big to ignore: the business case for Big Data. North Carolina: SAS Institute.

How to positively contribute to online society and promote equality and inclusion.

Xóchitl Elizabeth Méndez Sánchez

The evolution of Information and Communications Technologies (ICT) has favored the presence of new tools on the Internet, represented mainly by the existence of open spaces for communication and interaction.

One of the main elements to guarantee the effective enjoyment of the right to freedom of expression in digital environments is access to the Internet under equal conditions, which implies not only the possibility of having the infrastructure to access said environment, but also the implementation of public policies aimed at eradicating the digital divide, digital education and the elimination of barriers to its use and access; in such a way that access and spreading of information on equal terms is guaranteed, especially through positive actions aimed at people in vulnerable situations, without discriminatory treatment in favor of certain content on the Internet, to the detriment of those disseminated by certain sectors. (Maqueo, 2019)

Thus, the Internet has become a powerful tool for the exercise of human rights; it is an instrument that modifies the role played by other traditional media of social communication, such as radio, television and even newspapers. (Maqueo, 2019)

In recent years, the rapid advance of electronic media such as the Internet has constituted a global system for disseminating and obtaining information in various areas, including the government, since currently various authorities have institutionalized the legal possibility that some administrations citizens can carry them out through this medium, in favor of the efficiency of the provision of services and the value of time.

Therefore, one of the most important applications that Information and Communication Technologies (ICT) have offered is the possibility of modernizing public management through its use for the provision of services, the improvement of internal operations and the strengthening its relationships with citizens, companies, and other social groups, what has been called electronic government. (Coronado, 2021)

The evolution of Information and Communications Technologies has also favored the presence of new tools on the Internet, such as mechanisms that make information known, represented mainly by the existence of open spaces for communication and interaction; so, they have become one of the main elements to guarantee transparency, access to information and the effective enjoyment of the right to freedom of expression in digital environments, it has also managed to substantially reduce the costs of production, distribution and use of the information and the resulting content.

Currently, the active participation and growing number of users of social networks have produced important consequences in the exercise of some fundamental rights, such as freedom of expression and access to information. Expressing ideas in real time has become common; we are citizens immersed in a global world where we constantly interact through different social networks, especially when personal activities derived from daily tasks are disseminated: work, professional, opinions, reflections or some information of public interest.

In this way, having access to information is an essential pillar of democracy that, in addition to being a human right, can serve as an essential instrument for the exercise of other fundamental rights.

References

- Coronado, J. (2021). Electronic Government. Towards a humane, democratic and transparent technology. Continental University. Obtained from: https://repositorio.continental.edu.pe/bitstream/20.500.12394/10499/2/UC_Li_Gobierno_electronico_2021.pdf
- Maqueo,M(2019)https://www.sitios.scjn.gob.mx/cec/sites/default/files/publication/documents/201903/08_MAQUEO_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales.pdf

How it should be a communication mechanism between authorities and civil society so information reaches digital citizenship?

Amelia Lucia Martínez Portillo

The protection of personal data and people's privacy have been become two key rights for the development of a society that tends accelerated digitalization in practically all aspects of life daily life, being that, derived from the COVID pandemic, a large part of our activities had to be modified and adapted to the impulse of the new technologies that, although they already existed, became in some cases essential, from work issues, academics, procedures government, online shopping and recreational issues.

The digital environment can involve unprecedented risks for privacy, given the massive transfer of personal data and the information circulation by the owners, of an ever-increasing volume of information on a global scale in various platforms, thus weakening control over your personal data, which threatens civil and economic liberties, security, health, and even integrity of people.

In this sense, the authorities guaranteeing the right to data protection Personally, we have an arduous task of making citizens aware of how exercise their rights appropriately, so a fundamental task is the to sensitize citizens about its importance, mainly, in the digital world, in addition to knowing the mechanisms through which Guarantor Bodies, members of the National Transparency System, seek promote, disseminate and promote this human right of data protection personal, which is legislated in our Constitution and in various international instruments.

With this new digital environment in which it supposes, a range of opportunities, in economic issues, new forms of work, forms of creation and innovation, it must be considered that these developments technological and social also imply new challenges since there is no typicality and legal framework updated to the new reality. Therefore, the importance of generate the necessary reforms to adapt the regulations.

In this context we must remember that the human being must be at the center of technological evolution, and we cannot lose the sense of human rights for taking steps towards technological advances. The Guarantor Bodies have within our powers the Personal Data Protection, but in the face of these new advances we must raise awareness among citizens about their digital rights, since we have the fundamental task of making everyone aware of how to exercise them appropriately.

That is why promoting the Bill of Digital Rights of Users and Consumers should be one of the primary actions to enhance and improve the quality of life of every individual, in addition to raising awareness among the population about the risks and threats when navigating the digital world. "Nowadays, the protection of personal data is of great importance because we are transferring all the life that we had in the physical world, to the world digital, for the good of all, let us make technology our ally and let's take care of our personal data in digital environments."