JULY | 2023

GPA
Global Privacy Assembly

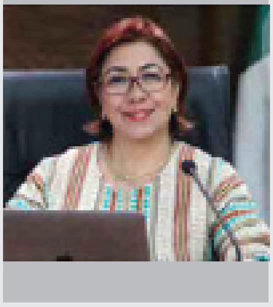
NEWS LETTER

AS THE WORLD BECOMES INCREASINGLY DIGITAL, PERSONALIZED ADVERTISING HAS BECOME UBIQUITOUS. **SHOULD BESPOKE BEHAVIOURAL ADVERTISING (BBA) CONCERN US?** BY MATTEO ZALLIO UX RESEARCHER AND ADJUNCT PROFESSOR, UNIVERSITY OF CAMBRIDGE

IN CONVERSATION WITH CONSTANZA GÓMEZ MONT, FOUNDER & PRINCIPAL OF C MINDS AND CLAUDIA MAY DEL POZO, FOUNDER AND DIRECTOR OF EON INSTITUTE ON ETHICS, OPPORTUNITIES, AND CHALLENGES OF IMMERSIVE AND EMERGING TECHNOLOGIES

CHAIRPERSON HAKSOO KO FROM THE PERSONAL INFORMATION PROTECTION COMMISSION, SOUTH KOREA ON THE NEED TO START INTERNATIONAL DIALOGUES ON ARTIFICIAL INTELLIGENCE.

MESSAGE FROM THE CHAIR



An ethical approach to the adoption of disruptive technologies involves a design that seeks to consider the needs, values, and experiences of human beings from the early stages of development.

When we talk about ethical principles in adopting emerging and disruptive technologies, we must consider certain fundamental principles, such as justice, which means ensuring that they benefit everyone, avoiding inequality and discrimination. Individual autonomy must be considered to respect freedom and people's capacity, allowing them to have control and decision-making power as users. It should do no harm, avoiding negative consequences and mitigate risks and dangers, and should be oriented towards the well-being and benefit of individuals and society.

Different technologies pose different ethical challenges. Artificial Intelligence is an example of this; for instance, Amazon and its algorithm for employment purposes, how can we ensure that the algorithm does not perpetuate unfair biases?

In cases like this, it is important to design transparent, explainable, and fair AI algorithms, and we must consider the human element and accountability to avoid completely delegating decisions that have ethical implications to machines.

An ethical application of emerging and disruptive technologies requires close collaboration among various stakeholders involved, from developers to political actors such as lawmakers and regulators. It is important to promote spaces for discussion and mechanisms for public participation that enable inclusion and decision-making.

However, ethical development and implementation of disruptive technologies is not enough without the work of regulators. How should governments respond to these technologies capable of triggering such rapid changes in our economies and societies?

It is of the utmost importance for us as Data Protection Authorities to understand the uncertainties and challenges that these technologies pose in terms of the social and economic relationships of our societies, and above all, their impact on the validity of the human rights we safeguard.

Therefore, to address the challenges posed by disruptive technologies, we need to apply a variety of policy tools to establish policy objectives, governance relationships, and norms within the sector.

Regulating disruptive emerging technologies emphasizes the need for regulatory frameworks that not only provide effective corrections to evident problems but also have anticipatory capacities that enable governments to identify and react appropriately to new challenges.

TABLE OF CONTENT

CYBERSECURITY IN DATA TRANSFER: PROTECTING INFORMATION IN A CONNECTED WORLD

BY: DANIEL MONASTERSKY | DATA GOVERNANCE LATAM

In the digital era, data transfer poses significant challenges in terms of cybersecurity and personal data protection. The global interconnectivity between Latin America and Europe and the widespread use of cloud services have led to an increase in cross-border data transfers. In this article, we will delve into the importance of cybersecurity in data transfer, focusing on the specific challenges organizations face when transferring data between countries in Latin America and Europe and when using popular cloud platforms. Additionally, we will examine best practices and key measures that organizations must take to ensure data security in this ever-evolving digital environment.

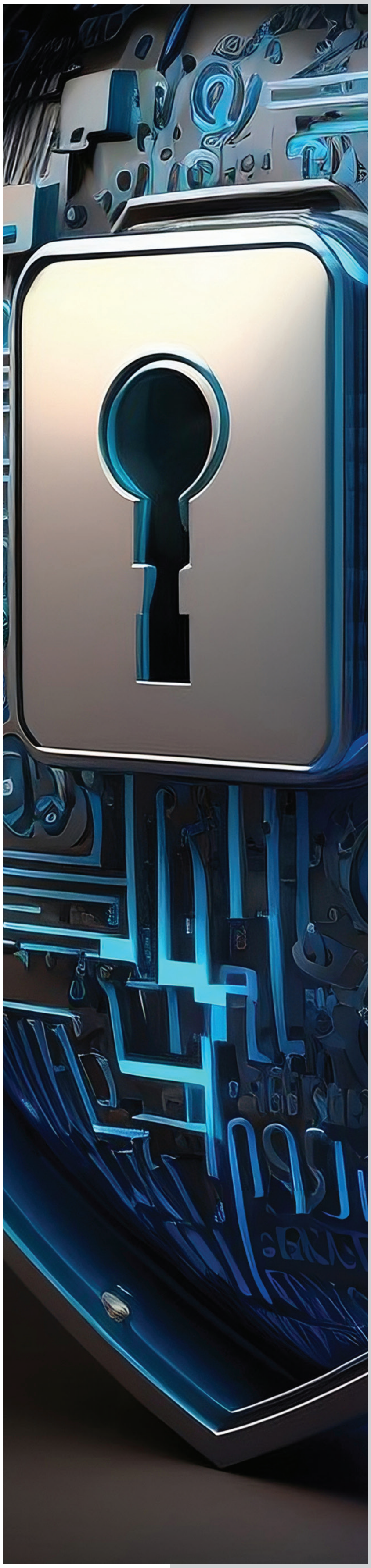
The legal framework and regulations in data transfer are fundamental to understanding how to protect information. Both in Latin America and Europe, there is a trend towards harmonizing data protection regulations, raising the bar in terms of security and privacy. The European Union's General Data Protection Regulation (GDPR) has set a global standard for data protection, and many countries are following suit by updating their data protection laws. In Latin America, several countries have enacted new laws or are in the process of doing so, reflecting a greater emphasis on the protection of personal data and privacy. This regional regulatory harmonization aims to ensure an adequate level of security and privacy for citizens and organizations, thus strengthening data protection in cross-border transfers.

Data transfer entails various risks and challenges in terms of cybersecurity. Common threats include unauthorized access, information theft, malware, and cyber-attacks. Additionally, the use of cloud services introduces potential vulnerabilities in data security. It is crucial for organizations to understand these risks and take proactive measures to mitigate them. This involves implementing robust security measures such as end-to-end encryption, multi-factor authentication, and constant threat monitoring. Clear security policies must also be established, and staff should be trained in proper security practices.

There are several best practices that organizations can follow to ensure cybersecurity in data transfer. Firstly, conducting a thorough assessment of cloud service providers before using them is recommended. This involves reviewing their security policies and practices, as well as their compliance with applicable regulations. Additionally, establishing access and privilege policies and regularly backing up data are essential. Adequate access controls should also be put in place, and staff should be trained in good security practices, such as using strong passwords and detecting phishing emails.
International cooperation is crucial in data protection and cybersecurity. Countries and organizations must work together to share information on threats and best practices, as well as cooperate in investigations and incident response. Moreover, there are international security standards, such as the ISO 27001, that provide a robust framework for cybersecurity management. Adopting these standards helps ensure that organizations comply with globally recognized security practices and strengthen their cybersecurity posture.

In the current landscape, data protection has reached a state of global maturity. Data breaches and growing privacy concerns have driven a significant shift in how data protection is perceived and managed. Organizations can no longer afford to ignore the importance of cybersecurity and regulatory compliance. Non-compliance can have serious consequences, including significant fines, reputational damage, and loss of customer trust. Furthermore, in an increasingly connected world, non-compliance with regulations in one country can have cross-border implications and hinder data transfer with other organizations and jurisdictions.

By understanding the legal framework, risks and challenges, and best practices in data transfer, organizations can ensure data security and strengthen the trust of their users in a global environment. The current level of maturity in data protection makes regulatory compliance an imperative. Organizations must recognize the importance of protecting personal and business data and take proactive measures to ensure compliance and strengthen their cybersecurity posture. Compliance with regulations is not only essential to remain competitive in a connected world where trust and data privacy are vital.



SHOULD BESPOKE BEHAVIOURAL ADVERTISING (BBA) CONCERN US?

USE OF BEHAVIOURAL AND BIOLOGICAL DATA TO CUSTOMISE ADVERTISING AND CONTENT IN DIGITAL IMMERSIVE ENVIRONMENTS:

DATA GOVERNANCE AND SAFETY CONCERNS

BY: MATTEO ZIALLO | UNIVERSITY OF CAMBRIDGE

Forecasts predict that by 2026 a quarter of the population will spend at least an hour a day in the metaverse or virtual or augmented environments[1]. This projection requires the consideration of several challenges and opportunities that will influence the design of the metaverse. Business leaders, CEOs, project managers, and DEI managers have a strong need to get inspired by new questions, concepts, and findings from scientific research.

As the world becomes increasingly digital, personalized advertising has become ubiquitous. One type of personalized advertising that has gained traction in recent times is Bespoke Behavioural Advertising (BBA). BBA is an approach and terminology developed at the University of Cambridge that utilizes behavioral and biological data to customize advertising and content in digital immersive environments, such as virtual and augmented reality[2].

[1] Gartner, 2022. Gartner predicts 25% of people will spend at least one hour per day in the Metaverse by 2026. https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026.

[2] Zallio M., Clarkson P.J. (2022). Designing the Metaverse: A study on Inclusion, Diversity, Equity, Accessibility and Safety for digital immersive environments, Telematics and Infor-matics, 2022, 101909, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2022.101909.

While BBA has the potential to provide a more engaging and relevant experience for users, it also raises concerns about data governance and safety.

What is Bespoke Behavioural Advertising (BBA)?

BBA is a type of personalized advertising that uses behavioral and biological data to create a unique and customized experience for users. BBA could support businesses to create personalized advertisement and offer users services and products answering their future needs. This type of advertising goes beyond traditional demographic targeting and instead targets users based on their behaviors, interests, and even physiological responses.

The Bespoke Behavioral Advertising (BBA) strategy predicts to be more effective than what is in place with current web cookies.

For example, if a user is browsing a virtual reality environment for running shoes, BBA technology can analyze their behavior and serve them advertisements for running apparel or accessories. This technology can also track a user's physiological responses, such as changes in heart rate or skin conductance or eye blinking, to determine their emotional response to specific content and serve them advertisements that align with their emotional state.

DATA GOVERNANCE AND SAFETY CONCERNS

One of the primary concerns with BBA is data governance. Behavioral and biological data are often sensitive and personal, and there is a risk that this data can be mishandled or even abused. BBA requires the collection and analysis of vast amounts of data, and this data must be managed and protected appropriately to ensure users' privacy and security.

Another concern is the potential for BBA to manipulate users' emotions and behaviors. If BBA technology can analyze users' emotional responses to content, there is a risk that it could be used to manipulate users' emotions to sell products or push certain agendas. This is a particularly significant concern when considering the potential impact on vulnerable populations, such as children or individuals with cognitive impairments.

BBA technology also raises concerns about algorithmic bias. If BBA algorithms are based on biased data or assumptions, they can perpetuate and even amplify existing societal biases. This can lead to discrimination or exclusion based on factors such as race, gender, or socioeconomic status.

Lastly, BBA technology has the potential to create addictive behaviors. By analyzing users' behaviors and responses, BBA technology can optimize content and advertising to keep users engaged and coming back for more. This can lead to addictive behaviors and even harm users' mental health.

REGULATORY AND ETHICAL CONSIDERATIONS

Given these concerns, there is a need for appropriate regulation and ethical considerations when it comes to BBA. In the European Union, the General Data Protection Regulation (GDPR) has been enacted to protect individuals' privacy and regulate the collection and use of personal data. The GDPR requires organizations to obtain explicit consent from users before collecting and processing their personal data, and it also provides individuals with the right to access and control their data.

In addition to regulation, ethical considerations are also necessary.

At the Metavethics Institute, a think-tank spun out from the University of Cambridge devoted to providing organizations with the right tools to sustainably tackle ethical and integrity challenges affecting digital, virtual, and immersive environments[3], studies on the effectiveness and ethical and integrity implications on using Bespoke Behavioral Advertising (BBA) advertising in virtual, augmented or mixed reality environments are carried on.

First discoveries shine the light on the aspect that to guarantee a human-centric Bespoke Behavioral Advertising (BBA) strategy there is a need to further create a universally agreed code of conduct helping to manage privacy, ethics and integrity across different virtual and immersive environments and raise awareness across the community by persuading businesses to develop informative tools based on shared principles.

CONCLUSION

To address these concerns, it is essential to establish strong data governance frameworks that protect user privacy and security. This includes implementing robust data protection measures, such as encryption, access controls, and data minimization strategies, as well as establishing clear guidelines and policies around the collection, use, and sharing of personal data.

It is also important to ensure that BBA is conducted in an ethical and transparent manner. This means providing users with clear information about how their data is being used and giving them the ability to opt-out of personalized advertising and content. Advertisers and content creators should also be required to adhere to strict ethical standards, such as those outlined in the General Data Protection Regulation (GDPR) and other privacy laws such as the California Privacy Protection Act (CPPA)[4].

In conclusion, while BBA has the potential to provide a more engaging and relevant experience for users, it also raises concerns about data governance and safety. Behavioral and biological data are sensitive and personal, and there is a risk that they can be mishandled or abused. BBA technology also raises concerns about algorithmic bias, emotional manipulation, and the potential for addictive behaviors.

[3] Zallio, M., Clarkson, P. J. (2023). Metavethics: Ethical, integrity and social implications of the metaverse. In: Tareq Ahram, Waldemar Karwowski, Pepetto Di Bucchianico, Redha Taiar, Luca Casarotto and Pietro Costa (eds) Intelligent Human Systems Integration (IHSI 2023): Integrating People and Intelligent Systems. AHFE (2023) International Conference. AHFE Open Access, vol 69. AHFE International, USA. http://doi.org/http://doi.org/10.54941/ahfe1002891

[4] Zallio, M., & Clarkson, P. (2022). Inclusive Metaverse. How businesses can maximize opportunities to deliver an accessible, inclusive, safe Metaverse that guarantees equity and diversity. Apollo - University of Cambridge Repository. https://doi.org/10.17863/CAM.82281

Given these concerns, at the Metavethics Institute we are eager to partner with organizations to support with assessment strategies of the ethical and integrity appropriateness of their advertisement and content development strategies.

IT'S TIME TO START INTERNATIONAL DIALOGUES ON ARTIFICIAL INTELLIGENCE

CHAIRPERSON HAKSOO KO | PERSONAL INFORMATION PROTECTION COMMISSION, SOUTH KOREA

ChatGPT arguably is the biggest buzzword in the technology sector right now. Since it was released for public access in late 2022, the large language model (LLM) trained by OpenAI has sparked keen interests as well as heated debates about artificial intelligence (AI) around the world. While certain share of the talks, frequently about generative AI such as ChatGPT, emphasize the benefits that AI is bringing to our daily lives, some observers argue that we need to pay close attention to the harm that AI could present to society. Concerns being raised include the risks that AI could pose to data privacy.

Already a number of jurisdictions have started responding to the concerns and, in some jurisdictions, discussions are under way for more concrete legislative measures. For instance, in the EU, the draft Artificial Intelligence Act, which was initially proposed in 2021, is currently going through legislative discussions. Some other jurisdictions, including South Korea, are also known to be taking steps toward possible oversight of AI. Still more discussions could take place to craft not just hard law but also soft law, in an effort to provide suitable guardrails to protect data subjects' rights.

There are competing views regarding the future prospects of technological developments surrounding AI. Those at one end of the spectrum argue that sophisticated AI systems could evolve to become a serious threat to humanity and that, as such, an immediate global regulatory response is warranted. While doomsday scenarios serve a clear purpose of sounding an alarm, however, it is not clear yet if there is sufficient scientific evidence to make an informed assessment about these scenarios. Regardless, it appears that certain types of risks, in particular related to data privacy, are increasingly becoming more apparent.

AI models are not without their flaws, and many rightly worry about their impact on society. One unmistakable characteristic of generative AI is that its output is plausible but often untrue. AI models may also facilitate social bias and discrimination, and they may be used as a tool for creating and spreading misinformation or disinformation. Lack of transparency is another key issue. Profiling, or the processing of various personal information to make generalizations about individual or group attributes, is also a concern. This can be coupled with automated decision-making by AI that may produce biased or incorrect results, and we are facing challenges in making the concept of explainability practicable. AI may also cause trouble by illegitimately exposing personal data if the data used in building the model is not adequately de-identified or anonymized. All these possibilities raise difficult questions regarding the way we process personal data in the age of AI.

These questions could eventually require revisiting and re-interpreting some of the fundamental principles of data privacy such as purpose specification and purpose limitation. Answering these questions is a daunting challenge and, in order to tackle the challenge, inputs from various stakeholders would be needed. Importantly, now that AI technologies are constantly evolving, a flexible and inquisitive attitude would need to be maintained in considering a response to the challenge. We propose the following perspectives, which could be considered in formulating a contour of future discussions.

First, we should carefully examine the essence of AI and its role in the social context. What are the workings of AI and how does it affect our society as a whole? What kind of influence can it have on individual data subjects? A systematic understanding of AI's impact on a broad social context should precede any attempt at reviewing and revisiting existing data privacy principles.

To narrow it down a bit, we could look into the role of personal data in AI model building and servicing. From the collection of data and use of training datasets to the deployment of the service, where and how does personal data fit into each of the stages? Is the data anonymized, pseudonymized, or otherwise transformed in any substantive manner in any of the development or deployment stages and, if so, what are the specifics? Only after being equipped with detailed understanding of this, could we evaluate the risk of AI unjustifiably exposing personal data or projecting distorted identities.

Second, we need to take into account the fast-changing nature of AI technologies. Advancements continue to take place at a breakneck speed and, once developed, AI-powered services are now released almost simultaneously in many parts of the world. Under these circumstances, an isolated and fragmented enforcement effort may not be very effective in addressing relevant risks. Instead, interoperable and harmonized responses among data protection authorities may be needed.

Third, efforts to create global standards and norms should not result in undue chilling effects on innovations. Rather, the framework for governing AI data should be shaped in a way that it encourages intriguing new experiments and innovations, while providing sufficient safeguards for data subjects.

Along with technological and social changes that AI is bringing to us, a daunting challenge is in front of us. It is time to start international dialogues in earnest.

ETHICS, OPPORTUNITIES, AND CHALLENGES OF IMMERSIVE AND EMERGING TECHNOLOGIES

Last week was a convoluted-week for privacy defense in the United States (US) as the American magazine Wired published two nerve-wracking stories. In the first, it exposed that certain US prisons were using new systems to track inmates down to their heart rates (Burgess, 2023), and in the second, it revealed that the US Government has been gathering troves of citizens' private informationfor over a year (Cameron, 2023). Unfortunately, the US is by no means the only country with such cases. As tech development and adoption continues without sufficient ethical and regulatory guardrails, these scenarios are destined to become regular occurences, typically impacting vulnerable groups the hardest. These stories should cause us to pause and reconsider what future we are enabling. As the global ecosystem moves towards updated or new privacy regulations, including the European Union's General Data Protection Regulation (GDPR), hailed as the golden standard for data privacy, new and intricate legal concerns are emerging based on recent tech developments such as the Metaverse, which has expert organizations wondering if privacy can still exist in such a world (Rosenberg, 2023).

Questions about the Metaverse, a hypothetical network of interoperable immersive virtual worlds powered by Augmented Reality (AR) and Virtual Reality (RV), really boil down to the latter two technologies and their enabling hardwares, given the Metaverse is still being collectively developed. AR refers to the use of digital mediums (from phones to tablets or headsets) to superimpose digital content on the physical world. In turn, VR refers to the use of digital mediums (headsets) to visually users into a virtual world. These technologies rely on a multitude of sensors to gather extensive and diverse data sets, and then use algorithms and automated systems to bring immersive worlds to life. The extensive data collection required for the functionality of these spaces is a leading concern for privacy defenders, as it may include intrusive information about users' facial characteristics, vocal attributes, eye movements, and ambient information pertaining to their surroundings, be it their home or office. The emergence of technologies such as electroencephalogram (EEG) sensors even makes it possible to detect user's unique brain activity through the scalp (Rosenberg, 2023).

AUTHORS:

CONSTANZA GÓMEZ MONT
FOUNDER & PRINCIPAL OF
C MINDS

CLAUDIA MAY DEL POZO
FOUNDER AND DIRECTOR
OF EON INSTITUTE

Without the appropriate safeguards, this data could potentially be exploited to manipulate users, engage in discriminatory practices, and make unfavorable decisions affecting both users and individuals in proximity (Future of Privacy Forum, n.D.). These concerns have not gone unnoticed: a recent survey on the Metaverse found that 50% of consumers are worried about user identity issues, 47% are concerned about forced surveillance, and 45% are considering the potential abuse of personal information (O'Neill, 2022).

Regarding user identity, the concern relates to the possibility of tracing virtual life activities and identities back to real individuals. Although users may generate avatars without disclosing personal information, complete anonymity is not a given. Information about their real-world identity could be inferred from behavioral or knowledge-based clues. This was the subject of an experiment by the University of Berkeley, which showed that the basic elements required for immersion (a headset and two hand controllers) gather sufficient simple motion data to uniquely identify a user in only 100 seconds with 94% accuracy. Moreover, this motion data can enable accurate identity deductions by integrating motion-based data with other commonly monitored data in virtual and augmented environments. While certain measures can be introduced to increase privacy, it would negatively affect the precision of physical motions, and thus users' experiences (Rosenberg, 2023).

The question of surveillance arises when one's privacy might represent a safety threat for other users, facilitating undetected harassment and discrimination, particularly pervasive among groups like women, PoC, LGBTQ+, and minors. According to online watchdogs, reports of women being sexually assaulted and harassed in the virtual reality worlds are increasing. The same can be said for other minority groups such as LGBTQ+ and BIPoC (SumOfUs, 2022), all challenges that have been occurring on social media platforms for well over a decade. While existing remedial mechanisms are far from satisfying (for example, there is widespread failure to take action against users who violate platforms guidelines), effective preventative mechanisms have been challenging to conceptualize. So far, the leading development in response to physical attacks is the personal boundary system, which keeps unauthorized users at a four-feet distance. It does not, however, cover other types of harassment.

The third biggest question surrounding privacy in immersive worlds is the potential misuse or abuse of personal information. Two challenges come together here, the first relating to the inherent vulnerabilities associated with transferring data between different immersive worlds, which could lead to data breaches and scams. It will be vital for platform operators and owners to agree on information security compliance, among other agreements that need to be reached (Wingarten & Artzt, 2022). The second challenge refers to the possibility to enter immersive environments from any location, which poses questions with regard to the limited jurisdiction of data privacy regulations. The same data and individual may fall under the jurisdiction of multiple privacy regimes simultaneously; yet, the field of privacy law has not fully adapted to the complexities of state and international boundaries, and it will likely take years before a consensus is reached (Weingarden & Artzt, 2022).

The challenges ahead are numerous and complex, and more than ever, stakeholders from all sectors must come together to explore and devise solutions to make the most of the profound socio-economic opportunities at stake, driven by these technologies. Research by Analysis Group suggests that, considering initial adoption of the Metaverse in 2022, it may contribute up to $3.1 billion USD to global GDP in 2031[1] (Christensen & Robinson, 2022). Experts that participated in a series of roundtables on the Metaverse organized by C Minds' Eon Resilience Lab and Meta in 2021 argued that it presented a unique opportunity to reduce inequality gaps, if done responsibly, supporting key priorities around the world such as health, education, and urbanism, to mention a few (Del Pozo & Rojas Arroyo, 2023). Use cases in these fields, as well as others such as female entrepreneurship and culture, for instance, are already showing how immersive technologies might improve people's lives when adopting ethical principles and a human rights a pproach in their design and implementation.

Unlocking these benefits in an inclusive and democratized way depends greatly on how proactive and intentional virtual world operators and owners, governments and other stakeholders across the world will be with regard to the development of responsible immersive worlds. Operators and owners should boost efforts for efficient collaboration mechanisms with users to co-design tools for experiences that are safe and mitigate human rights breaches. In turn, governments may need to pass new laws or update guidance on existing statuses, as stated by the Future of Privacy Forum's Senior Vice President of Policy (Uberti, 2022). Just as GDPR-like regulations were a necessary update to 1998's first data protection laws, another one may be needed sooner rather than later. These new regulatory developments should be carried out in innovative and collaborative ways; public policy prototypes could become increasingly popular tools to face the growing complexities of tech regulation. Moreover, stakeholders such as civil society and academia have the opportunity to advocate for ethical approaches through the development of standards and other efforts such as enabling education programs for people to understand both opportunities and risks.

While there is still a long road ahead, certain initiatives by nonprofit organizations stand out for their focus on inclusivity. In Latin America, a regional reflections series was put together for the public, working with over 40 local experts from 13 countries to explain what the Metaverse is, means, and might become in the region. In Canada, individuals that identify as First Nation are being offered free training to become developers and create solutions that respond to the needs of their communities, based on immersive tecnologies. In New Zealand, this technology is being used to preserve ancestral knowledge and culture, and support the economic self-determination of First Nation communities. In Nigeria, immersive technologies are being used to help create more empathy between individuals and communities. These are just a few examples of exiting initiatives across the globe.

Nearly 40 years after the invention of the Internet, the spark that created the base for today's far-reaching digital technologies, the world is a better place than it has ever been. Overall, that is. A more granular look will show that inequality is also at an all-time high. Humanity has learned, or so one should hope, that technology development is not automatically synonymous with the democratization of benefits. The promise of technology cannot end with the very few. What if this time we changed our approach? What if we made inclusivity, privacy and safety an intentional part of the design and development of these new immersive technologies?

[1] Measured in 2015 U.S. dollars

REFERENCES

Artzt, Matthias and Weingarden, Gardy. (2022). *Metaverse and Privacy*. International Asscoation of Privacy Professionals (IAPP). Accessed here: https://iapp.org/news/a/metaverse-and-privacy-2/

Burgess, Matt. (2023). *This Surveillance System Tracks Inmates Down to Their Heart Rate*. Wired UK. Accessed here: https://www.wired.co.uk/article/prison-wristband-talitrix-tracking

Cameron, Dell. (2023).*The US Is Openly Stockpiling Dirt on All Its Citizens*. Wired. Accessed here: https://www.wired.com/story/odni-commercially-available-information-report/

Christensen, Lau and Robinson, Alex. (2022). *The Potencial Global Economic Impact of the Metaverse*. Accessed here: https://www.analysisgroup.com/globalassets/insights/publishing/2022-the-potential-global-economic-impact-of-the-metaverse.pdf

Dan, Simmons. (2022). *17 Countries with GDPR-like Data Privacy Laws*. Comforte. Accessed here: https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws

Del Pozo, Claudia and Rojas, Arroyo Daniela. (2023). *Metaverso: Las oportunidades del futuro. Perspectivas desde América Latine y el Caribe*. Accessed here: https://www.metaversolat.com/_files/ugd/de03fd_4b69baf3d8474508a3423a4021a99be4.pdf

Future of Privacy Forum. (n.D.). *Immersive Technologies*. Future of Privacy Forum. Accessed here: https://fpf.org/issue/immersive-technologies/

O'Neill, Sarah. (2022). *What Privacy Issues Will Haunt the Metaverse?* LXA Hub. Accessed here: https://www.lxahub.com/stories/what-privacy-issues-will-haunt-the-metaverse

Rosenberg, Louis. (2023). *New research suggests that privacy in the metaverse might be impossible*. VentureBeat. Accessed here: https://venturebeat.com/virtual/new-research-suggests-that-privacy-in-the-metaverse-might-be-impossible/

SomeofUs. (2022). *Metaverse: another cesspool of toxic content*. SomeofUs. Accessed here: https://www.eko.org/images/Metaverse_report_May_2022.pdf

Uberti, David. (2022). *Come the Metaverse, Can Privacy Exist?* The Wall Street Journal. Accessed here: https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206

BETTER POLICIES FOR BETTER LIVES IN THE INCREASING DIGITALIZED WORLD

BY AMB. **HELENA SYBEL GALVÁN GÓMEZ** | OECD PERMANENT REPRESENTATIVE (MÉXICO)

In recent years, the speed at which the digital and technological transformation is taking place has intensified. Furthermore, the COVID pandemic served as an additional catalyzer to this already accelerated phenomenon.

Today, the digital transformation is embedded in almost every activity and interaction taking place in our societies. Our increasingly digitalized world provides us with additional tools to facilitate the way we relate in the different spheres of humanity. It affects the way we communicate, we learn, we do business, we access private and public services and products, we analyze and even how we design and implement public policies. These tools have an immense potential to bring great benefits and efficiencies to our societies and economies.

The digital transformation is also accompanied by risks and challenges. The capacity of countries to absorb, adapt and react to an increasingly digitalized world is not even. Advanced economies are better prepared to fully embrace the positive impacts of the digital transformation, while in the developing world the adoption of these technologies has exacerbated digital and non-digital inequalities and disparities across regions and countries.

According to the Organization for Economic Cooperation and Development (OECD) the term "digital divide" refers to the existing gap between individuals, households, businesses, and geographic areas at different socio-economic levels with regard to their opportunities to access information and communication technologies (ICTs) and to the use of the Internet for a wide variety of activities[1].

Governments have a unique opportunity to implement policies in order to better harness and bring the benefits resulting from this transformation to all. Last December, the key outcome of the OECD Digital Economy Ministerial was the "Declaration on a "Trusted, Sustainable and Inclusive Digital Future". This declaration sets out a vision for a human-centric and rights-oriented digital transformation.

In other words, we agree that everyone should have the same opportunity to access and benefit from the new digitalized world. Indeed, the digital divide cannot be understood merely with an economic efficiency rationale. It is critical to address the digital transformation with a comprehensive human-centric approach and prioritize digital inclusion as the foundation for everyone, including the most vulnerable, to participate, learn, explore, innovate, and benefit from the digital transition on equal terms. We can only maximize the digital economy's benefits if we also reduce social inequalities, leaving no one behind.

In order to materialize these benefits, access to digital and technologies has to be universal, and in order for it to be universal, the following is needed:

- More and better infrastructure: countries need to invest and deploy infrastructure in order to bring connectivity even to the most remote areas. A very important challenge in the developing world and in countries whose geographical characteristics make it very difficult to provide appropriate infrastructure.
- Higher network capacity and speed: connectivity is important but in order to reach and properly embrace the benefits of digitalization you need a minimum level of capacity and speed.
- Affordability: digital access should be seen as an individual right and not as a service to be bought and sold in the market.
- Skills: people need to have the relevant skills and education in order to be able to take advantage of this new tool.

In the case of Mexico, bridging the digital divide, including the gender gap will require important policy challenges. According to the OECD, internet and computer access in Mexico are more equal than access to education but more unequal than access to essential public services. In contrast, internet and computer access remain low compared to other OECD countries.

Substantial disparities persist in the use of the Internet across Mexico. According to the National Institute of Statistics and Geography of Mexico (INEGI), the percentage of households with Internet in 2020 varies greatly between states. In Mexico City, 80,5% of households have Internet, while in Chiapas, the figure is only 27.3%[2].

In order to bring connectivity and internet to all, but in particular to the most remote areas of the country, the Mexican government, in 2019, created a public company "*CFE Telecomunicaciones e Internet para Todos"*. It started using the electricity network to provide free telecommunications services and access to information and communication technologies, including broadband and the Internet. Now it is expanding the coverage through telecommunications infrastructure with 42,000 access points in clinics, public schools, governmental buildings and public squares and 24.000KMS of optical fiber. The goal by 2024 is to open access to 4.5G mobile networks for more than 20 million Mexicans located, mainly, in communities with fewer than 5,000 inhabitants.

Technological tools have the power of making our societies safer, better informed, freer. We must not forget that our goal in developing these technologies is to improve the lives of many and especially those who have been left behind in the past.

[1] OECD (2001-01-01), "Understanding the Digital Divide", OECD Digital Economy Papers, No. 49, OECD Publishing, Paris. http://dx.doi.org/10.1787/236405667766

[2] In Mexico, there are 84.1 million internet users and 88.2 million of mobile. ENDUTIH 2020. (2021, June 22). INEGI. Retrieved May 26, 2023, from https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTe-mEcon/ENDUTIH_2020.pdf

GPA

Global Privacy Assembly

NEWS LETTER

GLOBALPRIVACYASSEMBLY.ORG/NEWS-EVENTS/LATEST-NEWS

TWITTER.COM/PRIVACYASSEMBLY