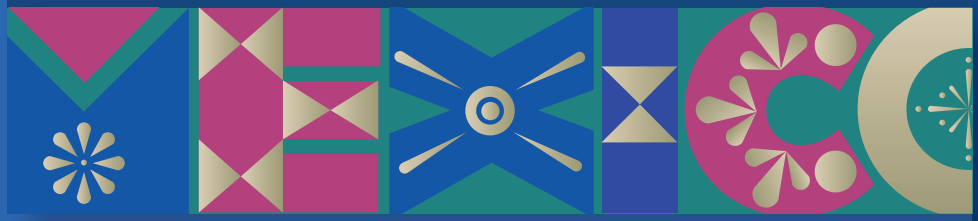
GPA

Global Privacy Assembly

43º Asamblea Global de Privacidad



18 - 21 OCT

MEMORY BOOK

INAI Mexico Host Commissioner 2021

Francisco Javier **Acuña Llamas**

Josefina **Román Vergara**

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

editorial jurídica sepin

GPA

Global Privacy Assembly

43º Asamblea Global de Privacidad

18 - 21 OCT

MEMORY BOOK

INAI Mexico Host Commissioner 2021

Francisco Javier **Acuña Llamas**

Josefina **Román Vergara**

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

editorial jurídica sepin

C/ Mahón, 8
28290 Las Rozas (Madrid)
Tel.: 91 352 75 51
www.sepin.es
sac@sepin.es

ISBN: 978-84-1388-211-6
Depósito legal: M-25171-2022

Producción gráfica: **sepín**, S. L.

Impresión: Grupo Espinosa

Table of contents

First part

Second part

Parallel Sessions

Third part

Audiolibro / Audiobook

First part

INAI Commissioners, Mexico

Dear experts, authorities, and civil society, on behalf of the Commissioners who make up the Plenary of the National Institute of Transparency, Access to Information and Protection of Personal Data of Mexico (INAI), it is a privilege for us to present the first compilation ever made of expert voices in data protection and privacy around the Global Privacy Assembly (GPA).

For several years, the GPA has played the role of a global summon bringing together authorities and key actors from around the world, organizing world conferences, identifying, and sharing good practices, and promoting and monitoring action plans to enable the global protection of personal data and its challenges, and above all, giving space and voice to international deliberations on the matter.

This compilation of experts' voices is based on the premise that privacy is an integral part of human dignity. As is known, the right to data protection was conceived as a prerogative to compensate for the potential erosion of privacy and dignity through the processing of personal data on a large scale, and in the digital age, we have gone through a cycle of evolution and exponential growth that has disrupted several areas of society: from the transformation of organizational processes, commercial activities, and production systems; even the means to communicate, inform and express ourselves; including how governments offer goods and services to the population.

The consolidation of the digital paradigm also means facing challenges of grand proportions, mainly when the data and information that we share through digital platforms, -which may include aspects of our most intimate and private spheres-, are improperly used and exploited by the State itself, non-state actors or even the private sector.

In this sense, we must continue generating a common lexicon so that regulators, companies, and citizens can identify innovative routes that allow us to mitigate these challenges by prioritizing a human-centered approach in our agendas, policies, and decisions through the protection, safeguarding, and security of personal information that circulates, without restrictions or barriers, through the ecosystems of the digital age.

Convention 108+ incorporates the concept of human dignity as individuals who are not treated as mere objects. The European Court of Human Rights also affirms respect for private life when referring to human dignity. By placing the human being at the center of data processing, technological developments are established to expand the human personality. While research shows that many people involved in online activities know that their

data is being collected and shared, this does not provide concrete evidence to assume that people are willing to share their data.

We live in the generation of data, so we have the right to determine what happens to it. Given technological advances, our ability to store and process vast amounts of data, and the evolution of artificial intelligence, business models increasingly view personal data as a suitable raw material for collection, refinement, and application for broader use. Even the paradigms of cross-border data flows and new digital rights are being debated in the highest spheres. By putting humans at the center of decisions, they can choose and/or accept the purposes for which their data is made available in a way that respects people's privacy.

The Internet and the global digital transformation have changed our lives. This new and emerging era in our history has influenced economies, communities, and people's personal lives. Human-centric approaches help societies ensure collective safeguards against potential data misuse and enable more opportunities for different sectors and groups.

Today we live in an ideal moment for proactive, interdisciplinary, and multisectoral collaboration since the accelerated adoption of a wide variety of technological tools, such as artificial intelligence, algorithmic programming, automated decision-making, blockchain or the analysis of large data, makes the ethical management of data imperative, as well as the creation of a robust, dynamic regulatory framework compatible with the best international standards, in favor of the protection and guarantee of human rights.

In this context, in the Forty-third edition of the Global Privacy Assembly, the most important forum for the protection of personal data and privacy worldwide, held in Mexico City from October 18th to 21st, 2021, and given the global context, the INAI, as hosting authority chose as the central theme **"Privacy and data protection: A human-centered approach".**

Holding this conference called for a collective effort of organization and participation in the context of the COVID-19 health pandemic. All of us who make up the Assembly understand that there is no time to lose on these issues; even the health emergency presented us with new challenges in terms of personal data protection and privacy, especially in handling data in the health sector. Technology allowed us this year, under a virtual scheme, to come together to share experiences, learn from each other, and propose practical solutions to the enormous daily challenges that face us.

The main objective of the 2021 edition of the Global Privacy Assembly focused on establishing international standards to guarantee the adequate safeguarding of the human right to privacy and data protection; providing new knowledge to guide the future of Data Protection and Privacy policies, achieving cooperation between authorities, and finding coexistence between the development of new information technologies and human rights for the protection of personal data. In addition to seeking the exchange of best practices, we intend to promote, as essential, an agreed action that is necessary for the world's citizens.

At INAI, the body responsible for protecting and guaranteeing the rights of access to information and protection of personal data in Mexico, we conceive our actions from an intersectoral and multidisciplinary perspective, as this is essential to generate greater

confidence among the population and thus take advantage of the benefits of the digital age for the benefit of society in general.

We encourage authorities and civil society to work more than ever on initiatives with a people-centered approach; let us remember that joint efforts will come together to respond to the immense challenges we face today. Democracy means that we must promote and protect human rights and fundamental freedoms, but it also means providing a better life for people.

With this edition, we want to promote new paradigms and ideas for innovation, maximize the use and protection of personal data, have better data availability for societies, explore data management and its potential, and finally, share visions and knowledge around the coexistence between the development of new technological tools and the protection of human rights to privacy and the protection of personal data.

INAI Commissioners, Mexico

Host Authority GPA 2021

Blanca Lilia Ibarra Cadena

Adrián Alcalá Méndez

Francisco Javier Acuña Llamas

Norma Julieta del Río Venegas

Josefina Román Vergara

History of the GPA

For four decades, the Global Privacy Assembly, first named the International Conference of Data Protection and Privacy Commissioners until the 41st Conference, has been the premier meeting place of the world's data protection and privacy regulators and enforcers. The Assembly has grown substantially, and its membership now extends across many parts of the world.

Each year the Assembly meets in a different city hosted by the local data protection or privacy authority. The Assembly first met in Bonn, Germany, in 1979 and then crossed the Atlantic for its second meeting in Ottawa, Canada. The Assembly met for the first 20 years in European locations with an occasional foray to Canada and one trip down-under to Sydney, Australia, in 1992.

From 2000 onwards, the Assembly arranged itself more formally to speak with one voice through joint statements. In Venice in 2000, the Assembly adopted guidelines and procedures for adopting Assembly resolutions "of enduring value" and followed this by establishing an accreditation process in Paris in 2001. In 2002 in Cardiff, the first 51 authorities were accredited. With the foundations in place, the Assembly was ready to adopt resolutions the following year.

In 2003 in Sydney, the first five resolutions were adopted on a mix of issues covering cross-border data transfers, technology issues, public communication of private messages, and data protection issues within international organizations. Today, the Assembly has adopted more than 75 resolutions and declarations.

With the increase in the size of the Assembly and greater expectations that regulators should become more effective at the global level, attention has been paid to Assembly organizational arrangements. In 2010, in Jerusalem, the Assembly established a five-member Executive Committee to provide leadership and ensure the attainment of the Assembly goals. Three years later, in 2013, in Warsaw, the Assembly formally adopted a mission statement and, for the first time, set out a strategic direction plan for the Assembly.

From late 2014 substantial efforts were undertaken to improve the Assembly's communications with members. Milestones included:

- A regular newsletter (2014).
- A website (2015).
- An alumni network (2015).
- An events calendar (2016).
- A Twitter account (2016).
- A YouTube channel (2017).

In 2015, the Executive Committee established a new transparent and competitive process for selecting hosts. Seeking to give effect to its 2016 resolution on developing new metrics of data protection regulation, the Assembly undertook the first census in 2017. That same year, the Assembly held its first awards program. The Global Privacy and Data Protection Awards recognized excellence and innovation amongst member authorities in research, enforcement, education, and online tools.

2021 marked a new beginning for the Assembly. The GPA focuses on enhancing regulatory cooperation to ensure its members deliver relevant regulatory outcomes, via collaboration, both within GPA and with global stakeholders, as they face new digital challenges and common global societal risks.

In 2021 the Executive Committee was formed by:

- Elizabeth Denham CBE, GPA Chair and UK Information Commissioner.
- Marguerite Ouedraogo Bonane, President of CIL, Burkina Faso.
- Angelene Falk, Information Commissioner at the Office of the Australian Information Commissioner.
- National Access to Public Information Agency (AAIP), Argentina.

Following the resignation of Eduardo Bertoni, the former director of the AAIP, the process of appointing a new director began, following the procedure provided by Law 27.275. In the absence of the Head of the AAIP and to continue the Argentinian participation at this

international forum, Mr. Eduardo Cimato temporarily continues the representation in his capacity as National Director of Personal Data Protection within the AAIP.

• Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information, Germany.

• Besnik Dervishi, Information, and Data Protection Commissioner, Albania (GPA Host 2019).

• The Board of the National Institute for Transparency, Access to Information, and Personal Data Protection of México. The Board of this Body is integrated by commissioners Blanca Lilia Ibarra Cadena. (INAI'S President), Francisco Javier Acuña Llamas (GPA works coordinator), Josefina Román Vergara (GPA works coordinator), Norma Julieta del Río Venegas and Adrián Alcalá Méndez.

• John Edwards, Privacy Commissioner, Office of the Privacy Commissioner, New Zealand.

After more than 40 years, the Assembly has more than 130 member authorities and many observers. It strives to achieve the vision of an environment where privacy and data protection authorities worldwide can effectively act to fulfill their mandates, both individually and in concert, through the diffusion of knowledge and supportive connections.

Former GPA Chair Elizabeth Denham, UK

Elizabeth Denham

Chair of the Executive Committee, Global Privacy Assembly 2018 - 2021
Former UK Information Commissioner

2021 marked the 43rd year of our assembly. The Global Privacy Assembly, and the ICDPPC before it, has a storied history, from our first meeting in Bonn, to the digital event held in very different circumstances last year.

Our story has many chapters, covering our assembly's formation, becoming truly global, and finding its place in the wider world. The most recent chapter has seen us evolve and modernize to meet the challenges of a data-driven age. We have found the strategy to give the GPA an effective voice, and the focus to make us relevant.

The completion of our 2019-2021 policy strategy and the confirmation of the focus for our plan for the next three years show what we can achieve together. As members we may be separated by borders and oceans, but legislation is becoming increasingly converged.

Through agreement and delivery of shared objectives, we can maximize our impact and relevance. That focus also enables us to confidently shape our story in the eyes of the wider community.

In 2021, we have completed the establishment of our external Reference Panel, led workshops with international organizations including the OECD and United Nations, and developed our ability to respond with one voice on key issues, including emerging issues in the Digital Economy, AI, and children's rights.

We have completed that work in the most difficult circumstances. This chapter of our assembly's story will be forever prefaced by the impact of a global pandemic, one that continues to present so many challenges.

As a community, we have responded to the challenge. Our COVID-19 working group continues to be an invaluable conduit for collaboration and sharing of expertise. Our new joint statements mechanism has enabled us to demonstrate the unity of our community on key issues.

As members, you shape our story. Some of you have helped to write the chapters already recorded. Others will be part of future chapters. I stepped down as chair of the Executive Committee in October 2021 enormously proud of the part of our story written under my stewardship. I am grateful for all of your support, and particularly the hard work and expertise of my colleagues on the Executive Committee. I am confident the Committee is well equipped to write our next chapter.

Former GPA Secretariat ICO, UK

Privacy is getting increasingly important in the digital age, so what can data protection and privacy authorities do to further uphold people's fundamental rights?

These were central issues under discussion as the Global Privacy Assembly joined together for their 43rd Closed Session in October 2021.

It was the honor of the Information Commissioner's Office, UK to provide the Chair and Secretariat for the GPA conference in 2021. Global pandemic challenges meant that we hosted the Closed Session online for our GPA members a second time.

The virtual conference was hosted by The National Institute for Transparency, Access to Information and Protection of Personal Data (INAI), Mexico, and brought together more than 90 members and observers to consider key data protection challenges. It followed an open session earlier in the week.

Opening the session, Elizabeth Denham CBE, outgoing GPA Chair and UK Information Commissioner, praised the work of the privacy community through the pandemic, calling for the Assembly to continue to be impactful.

Ms Denham said: "We were already in a data-driven age, even before the pandemic supercharged that acceleration of digital growth. Now data-driven innovation is helping us through health crises and influencing every facet of society.

"Our community's work is central to that, ensuring people trust that innovation. But we cannot assume that privacy will always have a seat at the table. Our input into discussions on key societal issues is dependent on an understanding that data protection and privacy supervisors bring a valuable insight, a practical mindset and we can respond promptly".

The **Closed Session balances features of both capacity building and policy,** both practically useful for GPA members. This featured two valuable policy-focused sessions:

• The first was dedicated to the topic of 'Data sharing – Innovation', featuring Keynote speaker Professor Helen Margetts, Turing Fellow and Director of Public Policy Programme at the Alan Turing Institute, and Professor of Internet and Society, Oxford University, UK.

• The Second was dedicated to 'Lessons Learned from COVID-19', led by Raymund E. Liboro, Privacy Commissioner/Chairman, National Privacy Commission, Philippines.

Resolutions were discussed and agreed at the conference, giving a shared view on a range of important current topics:

• Data sharing for the public good;

• Children's digital rights;

• Government access to data; and

• The future of the Global Privacy Assembly.

Other **capacity building topics** which support members' national work discussed in detail included international enforcement cooperation and regulatory sandboxes.

The Assembly also adopted a new strategic plan to guide its work for the next two years, committing to a continued focus on advancing global privacy, maximizing the GPA's influence and building capacity for members.

The Assembly also created the second edition of its **Member Census**, The GPA Census 2020 (published 2021) collected information from 70 members to provide a 'point in time' picture of the policies and delivery approaches that currently guide and regulate data protection and privacy globally.

The Census provides a useful reference tool for those whose business and data crosses jurisdictions and to national policy makers considering new legislative approaches. It also supports member authorities' capacity building and collaboration through dissemination of 'how it's done' in other jurisdictions.

The data in this Census informs the GPA's Working Groups which are responsible for delivering activity in support of the GPA 2019-2021 Conference Strategic direction and the successor document to follow.

The Global Privacy Assembly brings together more than 130 members and observers from around the world. **At the closed session, the following new members and observers were welcomed**:

New members:

• Commissioner of Data Protection, Abu Dhabi Global Market

• Office of the Queensland Information Commissioner, Australia

New observers:

• National Data Protection Authority (ANPD), Brazil

• Saudi Data and Artificial Intelligence Authority, Saudi Arabia

• Ministry of Transport and Communication, Qatar

• Data Protection Office, Qatar Financial Centre

• Privacy and Civil Liberties Oversight Board, United States

• Consumer Financial Protection Bureau, United States

• Asia Pacific Privacy Authorities (APPA) Forum

• Inter-American Institute of Human Rights (IIHR)

The results of the **2021 GPA Executive Committee election** were also announced:

• Marguerite Ouedraogo Bonane, from Burkina Faso's Commission for Information Technologies and Civil Liberties, stood down having completed her second two-year term; and

• Morocco's National Commission for the control and the protection of Personal Data (CNDP), was elected to the Executive Committee for a two-year term.

The GPA's Global Privacy and Data Protection Awards shine a light on the good practices delivered by the GPA Members in their respective jurisdictions. The Assembly announced the following winners in 2021:

• Education and Awareness: European Data Protection Supervisor

• Innovation: Commission Nationale de l'Informatique et des Libertés (CNIL), France

• Accountability: Information Commissioner's Office (ICO), UK

• Dispute Resolution and Enforcement: Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner of British Columbia, and Commission d'accès à l'information du Québec (Joint entry)

• People's Choice Award: Gibraltar Regulatory Authority

The 2021 Closed Session was another great GPA event to remember, and the former GPA Secretariat wishes to thank the INAI Mexico, and all involved in making the event a reality.

Second part

INAI Host Commissioners Coordinators

Francisco Javier Acuña Llamas and Josefina Román Vergara, Mexico

As INAI Host Commissioners Coordinators of the Global Privacy Assembly 2021 and on behalf of the plenary of the National Institute for Transparency, Access to Information and Protection of Personal Data (INAI)- which is the Mexican autonomous constitutional body that guarantees two fundamental rights: access to public information and the protection of personal data in both the public and private sectors by promoting a general culture of transparency and accountability of the government to society- we want to give our deepest gratitude to all the people who are part of this great collaborative work.

The Global Privacy Assembly (GPA) appointed its first Reference Panel, which is constituted as a group of 16 representatives from organizations from around the world, civil society, academic institutions, and privacy and data protection experts who share the vision and mission of the GPA. We thank the members: Clarisse Girot, Marc Rotenberg, Cecile De Terwangne, Masao Horibe, Eduardo Bertoni, Colin Bennett, Amber Sinha, Estelle Masse, Gabriela Zanfir-Fortuna, Andreas Mundt, Elizabeth Coombs, Bertil Cottier, Franziska Boehm, Valeria Milanes, Anne Cheung, and Bojana Bellamy, for being part of the organization.

This group, together with the organization's Executive Committee, helped generate this year's 2021 open session agenda by providing knowledge and practical experience on data protection and privacy, as well as brainstorming topics of interest for the audience related to cutting-edge technological developments.

The INAI served as a generator of opportunities for an open dialogue that allowed experts to discuss and exchange knowledge and ideas, and to propose solutions to emerging problems in the field. The agenda focused on the coexistence between new information technologies and human rights. The above was addressed through keynote speeches, panels, and parallel sessions where experts addressed their best practices.

We started the conversation with technological evolution and human intervention in massive data processing; Mass surveillance by facial recognition and metadata analysis; Privacy and Pandemic; Vaccination Passports and Similar Certificates; An Ethical Approach

to the Protection of Personal Data; Internet of Things. Likewise, topics such as artificial intelligence, digital rights, inclusive policies, and practical tools for free and secure data flow, among others, were addressed.

Experts triggered exciting conversations and debates related to the future of privacy and technology; The digital economy; The challenge of compliance; Normative convergence for the establishment of international standards for the adequate protection of human rights; The status of COE 108+; Consumer Rights; Electronic Commerce; Smart Cities and Mobility Hubs; poverty and marginalization; UN 2030 Agenda; Personal Data in the electoral field; among many others.

All these issues were of great interest to civil society and the authorities, as they gave rise to great conversations. Undoubtedly, the dialogue generated at the 43rd Global Privacy Assembly made it possible to include topics on the agenda that, although they may seem futuristic, they are present and, without due regulation and balance, could compromise our privacy.

We take this opportunity to thank Ms. Elizabeth Denham for all her guidance; the Reference Panel for all their hard work in jointly deciding the theme for this year's edition; the ICO Secretariat team that, with their daily work, made this possible; to all the authorities that, despite the complications of COVID-19, its work and contributions were reflected; to the civil society that accompanied us this year allowing us to hold an event of the highest level; and to the sponsors who without them we would not have been able to achieve this.

We are convinced that we are all co-responsible for closing the gaps and building democracy and governance in the international arena. Therefore, we must engage responsibly in decision-making and the generation of constructive knowledge to generate and promote actions and recommendations to protect personal data.

Francisco Javier Acuña Llamas

Josefina Román Vergara

Reference Panel

A human centric approach

Andreas Mundt

President of the Bundeskartellamt since 2009, member of the Bureau of the OECD Competition Committee since 2010 and the Steering Group Chair of the International Competition Network since 2013.

Some Thoughts on the Intersection of Data Protection, Privacy and Competition Law

The 43rd General Privacy Assembly particularly showed that privacy and data protection are no ends in themselves but have implications in many different areas. In my role as a member of the GPA Reference Panel, I perceive that it always has been an important concern of the GPA that supervisory authorities for privacy and other regulatory bodies are able to cooperate in order to enforce data protection rules in the economy. In my daily work as President of the Bundeskartellamt, the German competition authority, I see a substantial intersection of interests and activities for both competition authorities and data protection supervisory authorities. I am deeply convinced that we cannot turn a blind eye to this but have to think outside the box and also look at neighbouring areas of law. Due to the pivotal role of data in the digital economy, privacy and data protection considerations have become an increasingly important part of the work of competition authorities around the world in recent years. I am confident that, vice versa, the work of competition authorities helps data protectors to understand the data economy even better.

The Bundeskartellamt's Facebook case is a prominent example where privacy considerations were relevant for the finding of an abusive practice. The Bundeskartellamt found that Facebook's terms of service and the manner and extent to which Facebook collects, combines and further processes user data from different data sources without letting users choose to reject such unrestricted data processing amount to an abuse of dominance. In assessing the appropriateness of Facebook's behaviour under competition law, the Bundeskartellamt, considered the violation of European data protection rules – of course not without consulting the data protection colleagues – and imposed far-reaching restrictions regarding Facebook's processing of user data. In addition, the Bundeskartellamt is conducting several proceedings against other digital companies pursuing data-driven business models: For example, the Bundeskartellamt currently is investigating Google's data processing terms and Apple's app tracking rules.

International fora such as the GPA, and particularly the decision to establish the GPA Reference Panel, demonstrate the widespread consensus that many of today's challenges especially in digitalization can only be solved in an interdisciplinary manner. The International Competition Network (ICN), which may be seen as a counterpart to the GPA, also recognized the relevance of privacy and data protection consideration for the work of competition authorities and formed a project group on 'Competition law enforcement at the intersection of competition, consumer protection, and privacy' in 2020. The project group has published an interim report, which also concludes that the intersection of competition, consumer protection and data privacy considerations is becoming increasingly important in the context of a data-driven society. I am therefore confident that both data protection supervisory authorities and competition authorities will greatly benefit from each other's experience and expertise in the digital economy and in particular regarding issues related to data and privacy.

Como miembro del Panel de Referencia de la GPA, considero que siempre ha sido una preocupación importante que las autoridades supervisoras de privacidad y otros organismos reguladores puedan cooperar para hacer cumplir las normas de protección de datos en el entorno económico. En mi trabajo diario como presidente de la Bundeskartellamt, la autoridad de competencia alemana, veo una intersección de intereses y actividades entre las autoridades de competencia y las autoridades de supervisión de protección de datos. Estoy profundamente convencido de que tenemos que pensar más allá de la caja y mirar hacia la ley. Debido al papel fundamental de los datos en la economía digital, las consideraciones de privacidad y protección de datos se han convertido en una parte cada vez más importante del trabajo de las autoridades de competencia de todo el mundo en los últimos años. Confío en que, el trabajo de las autoridades de competencia ayude a los protectores de datos personales a comprender aún mejor la economía de los datos.

Anne S.Y. Cheung

Professor at the Department of Law, the University of Hong Kong Anne.cheung@hku.hk

We are living in an era of datafication wherein almost every aspect of our daily lives can be transformed into measurable data to be recorded, collated, evaluated, and sold by private companies. With the emergence of ever-advancing AI technology, this trend is being exacerbated. Now, choices (ranging from movies to partners) are being automatically recommended to us by online sites, profiles are built for us by data brokers and sold to unknown corporations, and even our recidivism tendencies are being predicted by the authorities. We unwittingly subject ourselves to big data analytics by voluntarily contributing information on a great variety of our lives to interconnected digital networks, thereby facilitating the corporations' and state's ability to profile and score us for the purposes of surveillance, punishment, evaluation, and exclusion. The relentless collection

of personal data and rampant advances in data technologies have culminated in a data ecosystem, powered by AI, carrying all its promises and perils.

In this data ecosystem, the famous saying —"We are data"— signifies the marginalization or even displacement of the "person". The data-selves risk redefining and overtaking our bio-selves. They are increasingly exerting direct impacts on the rights, interests, and even legal personality we enjoy in real life. Further, the ability of the mass-scale collection, analysis, and manipulation of data to determine the livelihoods and fates of individuals may lead to the emergence of a Data State, which is a governance model enabling the state to comprehensively monitor, evaluate, and control its subjects through datafication and data-driven techniques, leaving them with little room to assert their rights and defend their autonomy. Unsuspecting citizens who engage in various digital activities for gain and/or convenience may end up as docile subjects with no ability to choose to exit and/or resistance.

The end result is the bio-self's growing dependence on the data-self. There may come a point in time when refusal to participate in the data surveillance systems of business enterprises and the state means the denial of one's existence. Resistance becomes impossible, as one's livelihood and even survival have become inextricably intertwined with and dependent on the data-self dominated ecosystem.

Without recognizing the underlying danger of the relentless expansion of datafication leading to the bio-self being dominated or overtaken by the data-self, we may end up with a personal data protection regime without the "person". A human-centric approach to privacy and data protection is needed. Rather than data, we —the "persons"— have to be invited back at the center-stage. In devising a system of effective checks and balances for personal data protection, we must focus on the prevention of the emergence of a data-self dominated ecosystem.

Vivimos en una era de datificación, en donde casi todos los aspectos de nuestras vidas pueden ser trasformados en datos medibles para ser archivados, recolectados, evaluados, y vendidos por empresas privadas.

Esta recolección de datos personales y los avances en las tecnologías de la información han creado un ecosistema de datos que conlleva a un desplazamiento de la persona misma. Si no reconocemos el peligro de la expansión de la datificación que conduce a que el "yo" biológico sea dominado por el "yo" de los datos, podemos terminar con un régimen de protección de datos personales sin la "persona".

En lugar de datos, nosotros, las "personas", tenemos que ser invitados de nuevo al centro del escenario. Necesitamos un enfoque centrado en el ser humano para la privacidad y la protección de datos, y debemos centrarnos en la prevención de la aparición de un ecosistema dominado por los datos.

Eduardo Bertoni

First Director of the Access to Public Information Agency (AAIP) and Data Protection Authority, Argentina (2016-2020)

May privacy and personal data protection have an approach that is not centered on human rights? My answer is very clear. It is impossible since privacy is a human right recognized by international human rights treaties.

Regarding the universal protection of privacy, article 17 of the International Covenant on Civil and Political Rights (ICCPR) should be mentioned; and in the field of inter-American regional protection, the reference is to article 11 of the American Convention on Human Rights.

The UN Human Rights Committee, in General Comment No. 16, when interpreting article 17 of the ICCPR, explained that "[a]s all people live in society, the protection of private life is of relative necessity". It is also important to note that, despite not having an express mention of the right to privacy, the Human Rights Council in its resolution 28/16, highlighted that article 12 of the Universal Declaration of Human Rights and article 17 of the ICCPR they form the basis of such a right in international human rights law.

On the other hand, the American Convention on Human Rights gives article 11 the title "protection of honor and dignity" and does not mention the word "privacy" either. However, the article itself expresses a broad content in the field of protection when it refers to private life. This can be seen in the cases resolved by the Inter-American Court of Human Rights related to the protection of the home, the confidentiality of communications, reproductive autonomy, and sexual expression.

In other words, there can be no doubt that the right to privacy, even without being explicitly mentioned, is a fundamental human right, so it is up to the States to address it as such.

However, we could ask ourselves if when we talk about "privacy" on the one hand, and "personal data" on the other, we are talking about the same thing. I think not.

The lack of privacy protection violates the protection of personal data because our personal data integrates the concept of privacy. But, on the other hand, the lack of protection of personal data may be a problem only for one aspect of privacy. As we mentioned above, the interpretation of the Inter-American Court of Human Rights of the Right to Privacy covers many more aspects of our life than only our personal data.

Consequently, an arbitrary or abusive interference with personal data affects privacy and, therefore, affects a human right. Therefore, States also have an obligation to address the protection of personal data as a human right.

¿Puede la privacidad y la protección de datos personales tener una aproximación que no esté centrada en los derechos humanos? Mi respuesta es contundente. Es imposible dado que la privacidad es un derecho humano reconocido por los tratados internacionales de derechos humanos.

Sin embargo, podríamos preguntarnos si cuando hablamos de "privacidad" y de "datos personales" estamos hablando de lo mismo. Considero que no.

La falta de protección de la privacidad vulnera la protección de datos personales, porque nuestros datos personales integran el concepto relativo a la privacidad. Pero, por otro lado, la falta de protección de datos personales puede ser un problema solo para un aspecto de la privacidad. A manera de ejemplo, la interpretación de la Corte Interamericana de Derechos Humanos sobre el Derecho a la Privacidad, cubre muchos aspectos de nuestra vida y no únicamente nuestros datos personales.

Elizabeth Coombs

Affil. Assoc. Professor Department of Information Policy and Governance Faculty of Media and Knowledge Sciences University of Malta

A 'human centric approach' recognises human dignity —a concept firmly grounded in human rights—. Privacy provides and protects human dignity. While typically perceived as a right of the individual, the right to privacy also provides collective benefits. Recognising the right to privacy within law establishes boundaries preventing easy trespass upon personal space and communities.

In the age of data and debates on data protection regulation best able to meet the challenges of the digital era, it is easy to lose sight of the critical importance of the right to privacy to enabling autonomy and development of the person. Privacy and its informational expression as data protection, enables not just personal space or solitude, but the enjoyment of other human rights such as the right to practise one's faith, the right to freedom of opinion, and of assembly amongst other rights. This is particularly important for individuals in vulnerable situations and minority communities.

Data protection has important contributions to make to preserving the conditions for individual autonomy, and also for establishing "a zone where the State cannot readily trespass"1 that is, without lawful, necessary and proportionate purposes. Recognising and understanding the interactions between privacy and data protection, and between individual and collective benefits of human rights, are the bedrock of a human centric approach to privacy and data protection —an approach that provides individual and societal freedoms that comprise and buttress democracy—.

Un "enfoque centrado en el ser humano" reconoce la dignidad humana, un concepto firmemente arraigado en los derechos humanos. La privacidad proporciona y protege la dignidad humana. Si bien generalmente se percibe como un derecho del individuo, el derecho a la privacidad también proporciona beneficios colectivos.

Reconocer el derecho a la privacidad dentro de la ley establece límites que evitan la fácil trasgresión del espacio personal y de las comunidades. Reconocer y comprender las interacciones entre la privacidad y la protección de datos, y entre los beneficios individuales y colectivos de los derechos humanos, son la base de un enfoque centrado en el ser humano de la privacidad y la protección de datos; un enfoque que brinda libertades individuales y sociales que comprenden y respaldan la democracia.

Masao Horibe

Former Chairman, Personal Information Protection Commission (PPC), Japan. Professor Emeritus, Hitotsubashi University

Japan's Privacy Mark System

I would like to introduce Japan's Privacy Mark System as one of the human-centric approaches to privacy and data protection. It was originally based upon revised Guidelines for Personal Data Protection in the Private Sector issued by the Ministry of International Trade and Industry (MITI) in March 1997. I chaired the Working Group on Privacy to revise the 1989 MITI Guidelines.

Kanagawa Prefecture's PD Mark

As a result of my experience in Kanagawa Prefecture, which, with a population of some 9 million, is the second-largest regional government after the Tokyo Metropolis, I proposed that MITI should create a mark or seal of certification. The first ordinance on privacy at municipal level was enacted in Kunitachi City, Tokyo in March 1975, and the first at prefectural level was enacted in Kanagawa Prefecture in March 1990. In Kanagawa Prefecture, I was involved in drafting the personal information protection ordinance and proposing the introduction of a voluntary registration system for the private sector which is certified with the Personal Data (PD) Mark below.

I have been of the opinion that "personal data itself is the very essence of a living human" and that a higher level of protection is necessary to realize this idea.

(The "P" at the center denotes "personal", while the "D", for "data", surrounding it represents the protection of personal data.)

The PD Mark for the private sector in Kanagawa Prefecture was launched in 1990 and abolished in 2014. I checked applications from private enterprises as chair of the Kanagawa Council of Personal Information Protection for the Private Sector. While I do not have the exact figures, the number of registered organizations was more than 8.000.

Privacy Mark System launched in 1998

In July 1997, a JIPDEC (Japan Information Processing Development Center) committee chaired by me began discussions towards the realization of a mark or seal system as proposed by me. The Committee comprising experts and business-group representatives reviewed models for creating incentives for promoting data protection by providing some "mark" demonstrating the appropriateness of personal information handling. These efforts led to the creation and implementation of the Privacy Mark System on April 1, 1998.

Privacy Mark System

Privacy Marks have been granted to enterprises which have prescribed the compliance program (CP) conforming to MITI's Guidelines from April 1998 to March 1999 and JIS Q 15001 since April 1999.

(Privacy Mark registered as a trademark)

Under the Privacy Mark System, JIPDEC (now the Japan Institute for Promotion of Digital Economy and Community) and certain designated organizations (19 non-profit organizations as of June 2022) examine and assess applications from private enterprises. The certification is renewable every two years. Private enterprises assessed as appropriate have the right to display the Privacy Mark in the course of their business activities, for example, in pamphlets and advertising and on envelopes, letterheads, name cards, home pages, and such.

As of July 25, 2022, the number of Privacy Mark Entities is 17.050.

Kanagawa PD Mark abolished in 2014

In view of the expansion and market penetration of the Privacy Mark nationwide, I suggested in the early 2010s that Kanagawa Prefecture should abolish its PD system, remaining proud of its historically important role as an originator of the Privacy Mark. Kanagawa then did so in 2014.

Me gustaría presentar el Sistema de marca de privacidad de Japón como uno ejemplo de los enfoques centrados en el ser humano para la privacidad y la protección de datos. Originalmente se basó en las Directrices revisadas para la Protección de Datos Personales en el Sector Privado emitidas por el Ministerio de Industria y Comercio Internacional (MITI) en marzo de 1997. Me enorgullece mencionar que presidí el Grupo de Trabajo sobre Privacidad para revisar las Directrices MITI de 1989.

Como resultado de mi experiencia en la prefectura de Kanagawa, que, con una población de aprox. 9 millones, es el segundo gobierno regional más grande después de la metrópoli de Tokio, propuse que el MITI debería crear una marca o sello de certificación.

En vista de la expansión y la penetración en el mercado de la marca de privacidad en todo el país, sugerí a principios de la década de 2010 que la prefectura de Kanagawa debería abolir su sistema, y mantenerse orgulloso de su papel históricamente importante como creador de la marca de privacidad. Este hecho fue consumado por Kanagawa en el 2014.

Keynote Speech

Technological evolution: human intervention in mass data processing

Elizabeth Coombs's introduction to Jennifer King

Elizabeth Coombs

Affil. Assoc. Professor Department of Information Policy and Governance Faculty of Media and Knowledge Sciences University of Malta

Mass data processing has been implicated not only in the undermining of the right to privacy but other human rights as well, such as, freedom of opinion, freedom of assembly, freedom of movement amongst others.

Recognizing the significance of these encroachments, Dr King insightfully asked 'How do we regulate data at a societal level?'; 'What incentives do we create to encourage companies to care about data quality and ethical data collection practices?', and 'How do we encourage new models for data governance that prioritize individual and societal welfare?'.

I believe we should add to these questions 'What are State jurisdictions doing to protect individual and collective interests in privacy and data protection?' And, moreover, 'Do we need new models for data governance when ratified international human rights instruments already impose individual and societal welfare obligations?'

It is the duty of States parties to these international treaties to take up the human rights obligations they have committed formally to implement. The International Covenant on Civil and Political Rights (ICCPR), ratified by 172 countries, requires ratifying States to uphold these rights, including Article 17 (the right to privacy). This is coverage any new standard would struggle to match.

Governments' powers enable the setting of governance requirements which respect human rights as an integral part of doing business[1]. Under the UN Guiding Principles for Business

[1] Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 'Protect, Respect and Remedy: A Framework for Business and Human Rights' (2008) A/HRC/8/5 «Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 2008 A/HRC/8/5».

(UNGPs), States have an obligation to protect the human rights of all people within their jurisdiction from violations, caused either by their actions or omissions, or the acts of third parties, such as businesses. Protecting human rights against business- related abuse is, in most cases, a legal obligation upon States through their ratification of legally binding international human rights treaties. Notably, the UNGPs position business compliance as accountability rather than corporate philanthropy[2]. Applying international human rights law to mass data processing and its uses, such as AI, addresses the global nature of mass data processing.

Regulation and enforcement are powers of the State, and States 'bear the responsibility of respecting, protecting and fulfilling every person's human rights, it is their duty to ensure that private companies which design, develop or use AI systems do not violate human rights standards[3]'.

It follows that we also need to ask, 'Are governments doing enough to uphold their human rights obligations for privacy, and, if not, why not?'. A further question that comes to mind is 'What leadership is the privacy and data protection community prepared to take in asking States to meet their legal human right commitments?'.

El procesamiento masivo de datos se ha visto implicado no solo con el derecho a la privacidad, sino también con otros derechos humanos, como la libertad de opinión, la libertad de reunión, la libertad de movimiento, entre otros.

Reconociendo esto, la Dr. King en su intervención cuestiona: "¿Cómo regulamos los datos a nivel social?"; "¿Qué incentivos creamos para alentar a las empresas a preocuparse por la calidad de los datos y las prácticas éticas de recopilación de datos?" y "¿Cómo fomentamos nuevos modelos para el gobierno de datos que prioricen el bienestar individual y social?"

Creo que deberíamos agregar a estas preguntas: "¿Qué están haciendo las jurisdicciones estatales para proteger los intereses individuales y colectivos en materia de privacidad y protección de datos?" "¿Necesitamos nuevos modelos para la gobernanza de datos cuando los instrumentos internacionales de derechos humanos ratificados ya imponen obligaciones de bienestar individual y social? "¿Están haciendo los gobiernos lo suficiente para cumplir con sus obligaciones de derechos humanos en materia d e privacidad y, si no es así, por qué no?". Y otra pregunta que me viene a la mente es "¿Qué liderazgo está dispuesto a tomar la comunidad de privacidad y protección de datos personales para pedir a los Estados que cumplan con sus compromisos legales en materia de derechos humanos?".

---

[2] Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI' (Berkman Klein Center for Internet & Society, Harvard University 2020) «https://cyber.harvard.edu/publication/2020/principled-ai».

[3] 'Human Rights in the Era of Artificial Intelligence in Europe as a Setter of International Standards in the Field of Artificial Intelligence' *Council of Europe*, 20 January 2021.

Jen King, Ph.D

Privacy and Data Policy Fellow Stanford Institute for Human-Centered Artificial Intelligence. @kingjen

I was asked to talk to you about artificial intelligence and how we, as privacy experts and data protection professionals, should approach the question of how to regulate it. The question of how to regulate AI is one that we are all struggling with today – it is a complex topic with no clear answers. If AI is going to be part of our world, then how do we ensure it is implemented fairly, equitably, and does no harm? And of course, how do we also protect our data privacy?

What do we mean when we talk about artificial intelligence?

For consumers, this can mean many different things, if it means anything at all: smart speaker devices like Amazon's Alexa or Google Home; Smart robots; facial recognition technologies. Self-driving cars, and, of course, there are many more than just these examples. At the core of AI is the idea that we can build machines that can help us to achieve our objectives. This conception was developed by two Mathematicians in 1956, John McCarthy and Marvin Minksy, who convened one of the first gatherings to discuss the possibility of building AI: "Every aspect of learning or any other feature of intelligence can, in principle, be so precisely described that a machine can be made to simulate it. An attempt will be made to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves".

I find this definition notable for its confidence that we can so precisely define all aspects of learning that we can program machines to solve them. It takes for granted that there is a clear, objective reality that can be captured by logic. Yet one of the things we are learning about AI today is that while these systems can arrive at conclusions that may be logical but entirely lack common sense. Human-level common sense, in particular, is difficult to replicate.

What do we mean by intelligence when we talk about artificial intelligence?

Stuart Russell, a professor of computer science at UC Berkeley, argues that intelligence is dependent not only on a set of goals but also on a form of input. According to Russell, "An entity is intelligent to the extent that what it does is likely to achieve what it wants, given what it has perceived". The relationship between specifying a goal and accomplishing it depends on how we frame that perception – how we describe the boundaries of the purpose, establish what constitutes success, and identify a set of valid outcomes.

However, how AI "learns" its intelligence –how it distinguishes between outcomes– depends on its training data. All forms of AI must start with a set of data from which it develops its "understanding" of the problem space. Here's an example on an AI trained on a dataset composed of online photos and their nearby text on webpages. This AI has determined this image: "A cat sitting on a chair with its paws tucked up underneath it" –that this is a loaf of bread, not a cat–. Note that the AI is 97% certain that this is a loaf of bread. AI can be incorrect even when it possesses a high degree of certainty.

It is important point out that AI is both very fallible and dependent on the data its fed. Even if you have trained an AI thousands of images of cats, it still may conclude that this image contains a loaf of bread.

Defining intelligence is not a straightforward or settled issue. None of us should accept that AI will categorically be "more intelligent" or will automatically be an improvement over humans at any particular task. Dan Hendrycks, a researcher at UC Berkeley, notes that "It's unpredictable which problems artificial intelligence will be good at, because we don't understand intelligence itself very well".

In order to understand AI, we need to understand algorithms. Algorithms are a precisely defined method for computing something or solving a problem. A set of instructions. Algorithms define the decision space in which a system works. All computing, including AI, requires algorithms. A difference between traditional computing and AI is that AI systems use pattern matching and statistical methods to make predictions to solve specific problems. The critical component that determines how successful any AI system is in predicting or learning is training data -- what data was used to create the decision space for a specific AI.

There is a famous saying in computer programming: garbage in, garbage out. This is as true for AI as in any other computing context. AI is only as good as the data used to train it. Yet, in public discussions about AI, we see very little focus on issues of data and lots of focus on algorithms. Given how important data is to AI, I think that understanding and regulating its contribution is of the utmost importance and one area where data protection authorities can have a major impact on what kinds of AI is built and how it impacts both individuals and societies.

My concern with data leads me to two key questions: First, what incentives can we create to encourage companies to care about data quality and ethical collection practices? Second, how can data protection authorities regulate AI through data? I want to talk about both incentives and regulations because I think it's important for us to discuss what practices we would like to see adopted, and consider what aspects of these problems could be addressed through strategies that don't exclusively focus on regulation.

Let me discuss this in terms of the current state of affairs here in the US, which I think is a very negative example!

Let us consider the case of the company Clearview AI, which has created an enormous database of facial images they have taken from every part of the Internet that they can access to develop a tool for international law enforcement agencies that IDs individuals through facial recognition. Here in the US, they face multiple lawsuits over their data collection practices and given our lack of data protection regulation, they may prevail despite their unethical practices. However, I would suggest that even though how they have gathered this data is unethical and potentially illegal, given their options, it is rational. Our absence of data protection regulation, combined with a lack of access to data and potentially high costs of obtaining it, creates a situation where taking the data without permission is a logical business strategy.

The question is not just how we prohibit these types of uses of AI, but how do we disincentivize these data practices? How do we change this? I suggest that in addition to regulation, which I will discuss next, we need to think about how to shift the data ecosystem into one where the path taken by Clearview is not the one that makes sense, where companies are incentivized to act ethically and to prioritize quality.

There are benefits to collecting & sharing data, but how do we incentivize companies to do so ethically? Providing positive data incentives may not solve all that ails AI, but data does contribute to issues of bias, discrimination, unfairness, and human rights violations. Some of the positive incentives I am considering are:

• Rethinking data infrastructures & standards to support more control over data.

• Encourage culture shift towards safety at large tech companies.

• Incentivize use of emergent methods/tools for data accountability, addressing data quality/provenance issues.

In terms of regulation, we need to think about how we can influence the data used by AI through data protection rights for individuals.

Some countries are much farther ahead on this issue than others; here are some suggestions. In terms of regulating AI through individual rights, I do think the Fair Information Practice Principles of consent, purpose specification, and correction and deletion (especially deletion by default!) play role. We also need to consider how to respect one's right to refuse to collection, and how to withdraw consent. A core challenge is how to change the data ecosystem to put real control into the hands of individuals

Thinking beyond how we regulate data at the individual rights level, I encourage you to consider how to regulate data at a societal level in order to consider the impact of data on us collectively, not just individually. Will this data contribute to negative impacts on privacy for society as a whole, not just the individual? In particular, I suggest that we consider: ethical data collection rules that consider impacts on society (harms outside of individual control); prohibiting/restricting some data types for commercial use; and investment in public sector data sources for noncommercial uses. A challenge is acknowledging that there are data problems individual rights don't solve.

Finally, in thinking about data governance and oversight broadly, how do we turn the data ecosystem on its head and create the infrastructure that would allow us to force large platforms to divest their data? This is the issue that antitrust and competition regulators may not be able to solve —in many cases—, breaking up these companies won't solve the data issues I've discussed. We need to ask ourselves: how do we encourage new models for data governance that prioritize individual and societal welfare? I recommend several data accountability measures: a shift away from data monopolies (divestiture); data provenance (documenting proof of origin, ethical collection, and permission to reuse); and, supporting the creation of data intermediaries to help consumers manage their data. The challenge here is that these measures require new standards and legal constructs to build out.

To conclude, I want to restate that while algorithms are important aspects of AI, AI is impossible without data. And we should not assume that AI is an appropriate tool for all of the problems we try to use it for. As we are already seeing, there are many instances where the data companies use is simply not adequate. If we are to allow AI to be used in our societies, it must start with data that is fit for purpose. You can't make good AI from bad data.

Finally, while the ideas I have shared with you are some approaches that I have been considering, I welcome your feedback and your suggestions as how to improve these approaches.

Thank you for your time.

Me pidieron que les hablara sobre inteligencia artificial y cómo nosotros, como expertos en privacidad y profesionales en protección de datos, deberíamos abordar la cuestión de cómo regularla. La cuestión de cómo regular la IA es algo con lo que todos luchamos hoy; es un tema complejo sin respuestas claras. Si la IA va a ser parte de nuestro mundo, entonces, ¿cómo nos aseguramos de que se implemente de manera justa, equitativa y no dañe? Y, por supuesto, ¿cómo protegemos también la privacidad de nuestros datos?

Definir la inteligencia no es un tema sencillo o resuelto. Para entender la IA, necesitamos entender los algoritmos y los datos. Mi preocupación por los datos me lleva a dos preguntas clave: primero, ¿qué incentivos podemos crear para alentar a las empresas a preocuparse por la calidad de los datos y las prácticas éticas de recopilación? En segundo lugar, ¿cómo pueden las autoridades de protección de datos regular la IA a través de los datos?

Quiero reiterar que, si bien los algoritmos son aspectos importantes de la IA, la IA es imposible sin datos. Y no debemos asumir que la IA es una herramienta apropiada para todos los problemas para los que tratamos de usarla. Si vamos a permitir que la IA se use en nuestras sociedades, debe comenzar con datos que sean adecuados para su propósito. No se puede hacer una buena IA a partir de datos incorrectos.

Las ideas que he compartido con usted son algunos enfoques que he estado considerando, agradezco sus comentarios y sugerencias sobre cómo mejorarlos.

Privacy and Pandemic COVID-19: Vaccine Passports and similar certificates

Elizabeth Denham's introduction to Alessandra Pierucci

Elizabeth Denham

Global Privacy Assembly Chair 2018-2021

Welcome to this session, looking at privacy and COVID-19 vaccine passports.

In my opening earlier today, I proposed we keep two questions in mind through our conference. Do we understand how people feel? And how does privacy stay relevant?

There can be no topic where this is more relevant than around COVID vaccine passports.

The need to understand how people feel about schemes that can rely on the sensitive health information of entire populations seems clear.

But what is less straightforward is how privacy stays relevant when the stakes are so high. That is the challenge so many of us have faced over the pandemic.

How do we make sure privacy is considered in schemes that are so integral to reopening society, to lifting restrictions of civil liberties and travel, and to revitalizing economies?

Alessandra Pierucci is well placed to discuss these challenges.

As chair of the Committee of Convention 108, Alessandra has a unique insight, informed by her involvement with a treaty that lists more than 50 signatories through Europe and beyond.

She also has a vast experience of data protection, as a lawyer, a regulator and as a contributor to the EU's Article 29 Working Party.

Alessandra, the microphone is yours.

En mi discurso inaugural, propuse que tuviéramos dos preguntas en mente durante nuestra conferencia. ¿Entendemos cómo se siente la gente? ¿Y cómo la privacidad sigue siendo relevante?

No puede haber un tema en el que esto sea más relevante que en el entorno relacionado a los pasaportes de vacunas COVID-19. La necesidad de comprender cómo se siente la gente acerca de los esquemas que pueden basarse en la información de salud sensible de poblaciones enteras parece clara. Pero lo que es menos sencillo es cómo la privacidad sigue siendo relevante cuando hay tanto en juego. Ese es el desafío al que muchos de nosotros nos enfrentado durante la pandemia.

¿Cómo nos aseguramos de que la privacidad se considere en esquemas que son tan integrales para reabrir la sociedad?, ¿Cómo levantar las restricciones de las libertades civiles y los viajes, y revitalizar las economías?

Alessandra Pierucci está más que calificada para discutir estos desafíos.

Alessandra Pierucci

Chair of the Council of Europe Consultative Committee of Convention 108

There are numerous angles, questions, ethical issues raised by the measures adopted by States to contrast the Covid-19 pandemic, including in respect of the initiatives of many regulators to issue certificates that prove the immunization and good health of people.

We are approaching our second year of coexistence with the pandemic and many questions still animate the debate, such as: are certificates a tool to regain our liberties and rights or could they trigger unbearable forms of discrimination and widespread surveillance? Which liberties and rights are we talking about, to health, to travel, work, attend cultural or leisure events?

The answers to these questions are not in the hands of the SAs solely. These questions are intertwined with a considerable number of other issues, related for example to the vaccine distribution in the world and forms of vaccine nationalisms which create a global inequality between countries thereby producing seclusion and discrimination of more vulnerable people.

Provided that the ethical and legal questions raised by certifications go beyond a pure data protection assessment, the main issue I would like to focus on is: how do we ensure the proportionality between the measures adopted and the protection of personal data?

There are some elements that can facilitate the achievement of this proportionality. First, as we know, the setting up of such certificates must be provided for by law.

Recommending that a legislative act accompanies the introduction of these measures is however essential but not enough.

A high quality of the legislative tool must be ensured. Meaning, first of all, that an accurate impact assessment must proceed the introduction of such certificates, to evaluate the repercussions of the measures being adopted as well as the effectiveness of already existing less intrusive measures. In data protection language, we would speak about a *data protection impact assessment*, but it's becoming clearer and clearer that such evaluation is intertwined with a more comprehensive *human rights impact assessment*.

A high-quality legislative measure also means that the legal basis must provide an explicit indication of the specific purposes pursued, a clear reference to the range of authorities and public and private bodies allowed to access the data contained in the attestation, to the categories of data concerned, as well as to the scope of the access authorizations.

What should be kept in mind is that the adoption of legislative measures, far from being a mere formalistic fulfillment, is an opportunity to implement data protection requirements such as:

1. minimisation: we don't need so many data for the correct functioning of the certificates. Personal data necessary to identify the data subject; unique identification of the certification; date of end of validity of the certificate are enough to ensure the proper functioning of the certificate. Moreover, the certificate should be based on a unique model without revealing the different reasons why it has been obtained (e. g. vaccination, exemption from vaccination, healing, negative test). Passports revealing vaccination exemptions may be used for example in some workplaces and reveal very sensitive data on the worker's health to the employer.

2. transparency: being aware that transparency is also a question of trust and acceptability, the law should indicate the specific purposes pursued, the features of the processing and those who can process the data collected in relation to the issuance and control of certifications.

3. specific data retention periods and security and privacy by design measures; this, having in mind that, although this is not a novelty of the current health crisis, the contrast to the pandemic has triggered public and private partnerships which deserve the highest attention in order to prevent the exposure of critical/sensitive information related to individuals to purposes not legitimately expected by the data subjects.

In the assessment of the elements I have just recalled, supervisory authorities (SAs) have a crucial role to play. The urgency of the measures to be adopted by governments cannot become a reason to avoid the involvement of the SAs, which are keen to provide their prompt contribution.

The intervention of supervisory authorities, during the preparation of a legislative act is not only a necessary procedural step to render the legislative act legitimate: a) it is fundamental for the Authority to present appropriate methods and respecting data protection principles from the design stage; b) it is in the interest of governments whose political choices would be supported by the expertise of supervisory authorities on such delicate and technical issues.

There are two considerations that have been identified from the very beginning of the debate on the correct balancing between the need to contrast the pandemic and the preservation of human rights and that still remain central to the discourse.

The first one is that alternatives to the vaccination should be ensured as much as possible in order not to transform the request for a Covid pass into an indirect obligation of vaccination.

The importance of alternatives, which was identified as a priority by the data protection community from the very beginning has proven to be crucial, and still very relevant especially considering that certificates can be used not only to facilitate a safer free movement among different states, but also for additional purposes.

And I go now to the second element: when assessing the proportionality of the measures taken to contrast the pandemic while keeping a high level of protection of fundamental rights, the measures adopted must by of *temporary nature* and part of a coherent and efficient health strategy.

The need to reassess the necessity of extraordinary measures was indeed considered since the first measures against the pandemic were taken (confinement, contact tracing, etc.) and is reaffirmed today when the evolution of the pandemic has brought us to the need to attest our Covid status. This is a challenge on which our attention must remain high as there is always the temptation to perpetuate measures which were thought for extraordinary circumstances only, and because there is always a new emergency lurking the horizon.

To conclude:

Giovanni Buttarelli —whose vision has been an incredible example for all of us and who believed in and supported the potential of the GPA— used to say that personal data tells a story about the individual which, in the best case scenario, would be used for the common good, but in the worst may act as a boomerang against them.

If we apply his words to the current scenario, we will say that the story about the person told by personal data regards her health, the common good would be the preservation of public health, but also other fundamental rights, as the boomerang here, to say with Giovanni's words, is discrimination, surveillance, and a profound attack to democracy.

It's precisely against these risks that all parties must keep their attention high and engage in the construction of an appropriate balance between the need to preserve the health of people and the protection of self-determination and equality.

Only in this way, the attempts to fight against health crisis, including vaccine passports and attestations, will not appear as an unreasonable and unacceptable means of limiting fundamental rights and can become a way to "restart" the effective enjoyment of the rights suspended during the pandemic.

Nos acercamos a nuestro segundo año de convivencia con la pandemia y muchas preguntas aún animan el debate, como: ¿son los certificados una herramienta para recuperar nuestras libertades y derechos o pueden desencadenar formas insoportables de

discriminación y vigilancia generalizada? ¿De qué libertades y derechos estamos hablando, a la salud, a viajar, trabajar, asistir a eventos culturales o de ocio?

Las respuestas a estas preguntas no están únicamente en manos de las autoridades. Estas preguntas se entrelazan con un número considerable de otros temas, relacionados por ejemplo con la distribución de vacunas en el mundo y formas de nacionalismos de vacunas que crean una desigualdad global entre países, lo que produce reclusión y discriminación de las personas más vulnerables.

Dado que las cuestiones éticas y legales que plantean las certificaciones van más allá de una mera evaluación de la protección de datos, la cuestión es: ¿cómo aseguramos la proporcionalidad entre las medidas adoptadas y la protección de datos personales? La legislación debe procurar la minimización de datos, la transparencia y un diseño para prevenir la exposición y mal uso de datos personales.

Data Flows with Trust

Jonathan Mendoza's introduction to Mieko Tanno and Bruno Gencarelli

Jonathan Mendoza Iserte

Secretary for Personal Data Protection at INAI Mexico
@JonnhyMendoza

We are part of a digital generation that uses technology to develop our daily activities, including commercial transactions through internet devices, which empowers the digital economy with data. Digital products and services acquired from different countries are part of our reality. In a world dominated by technological innovation and internet connections, we face various risks that jeopardize our integrity.

In this regard, I would like to comment on two specific points regarding data flows: firstly, the necessity to have clear regulations that do not endanger our integrity nor suppress innovation, efficiency, and economic activity; and secondly, the need in Latin America to create a regional instrument with standards of data protection that allows data flows.

Firstly, as digital users, we must be sure that our personal information is safeguarded under the highest standards of personal data protection and privacy rules; this depends on how governments manage the privacy of their citizens, which has a strong cultural component. Even though international harmonization is extremely difficult because each country has a different approach to data protection and data trust, we must ask ourselves: can governments minimize barriers to cross-border data transfers to address common challenges and benefit society?

The creation of trust between governments is needed to achieve regulatory cooperation, but also, we need to think about which guarantees as citizens we should demand from personal data protection authorities and technology developers.

As we have seen in recent years, the enforcement of the standard contractual clauses for data transfers between the EU and non-EU countries allows a free data flow by providing protection and confidence to the data users, and it ensures that the cross-border free flow of information and e-commerce operations are more dynamic. As we will see in the following presentations, examples of the contractual clauses model introduced in Japan by Commissioner Tanno and the European Commission by Bruno Gencarelli allow free data flow with trust among commercial regions.

Secondly, I take this opportunity to stretch out the necessity to establish a Latin American standard of regional data flows. Even though, it exists the "Standards for Personal Data Protection for the Ibero-American States" and the "Updated Principles on Privacy and Personal Data Protection" of the Organization of American States (OAS), it is still a long way to create an instrument that allows standardization in the region.

This regulation should set a minimum protection standard that does not obey the international instruments but rather address sociocultural topics of the region, maintain an open-door policy to international cooperation with other data protection authorities, and have clear regulations on private-public relationships. We can start by doing practical exercises through sandboxes or open loops that will set the foundations for a correct regulatory implementation conveying the maturity and culture of each society.

Somos parte de una generación digital que utiliza la tecnología para desarrollar nuestras actividades diarias, incluidas las transacciones comerciales a través de dispositivos de internet, lo que fomenta la economía digital. En este sentido, me gustaría comentar dos puntos específicos con respecto a los flujos de datos transfronterizos: primero, la necesidad de contar con regulaciones claras que no pongan en peligro nuestra integridad ni supriman la innovación, la eficiencia y la actividad económica; y en segundo lugar, la necesidad en América Latina de crear un instrumento regional con estándares de protección de datos que permita el libre flujo de datos.

Es necesaria la creación de confianza entre los gobiernos para lograr la cooperación regulatoria, pero también debemos pensar qué garantías como ciudadanos debemos exigir a las autoridades de protección de datos personales y a los desarrolladores de tecnología.

La regulación latinoamericana propuesta debe establecer un estándar mínimo de protección de datos personales transfronterizo que no obedezca a los instrumentos internacionales sino que aborde temas socioculturales de la región, mantenga una política de puertas abiertas a la cooperación internacional, y cuente con normas claras sobre las relaciones público-privadas.

Mieko Tanno

Chairperson, Personal Information Protection Commission, Japan

"The concept of DFFT"

Due to a rapid increase in use of data in the world along with the COVID-19 pandemic, the environment surrounding digital data has been changing dynamically.

Since the legal systems related to data flow differ from country to country reflecting its history, national characteristics and political systems, policy coordination is essential for free flow of data across borders.

«What is DFFT?»

Japan advocated the idea of Data Free Flow with Trust (DFFT), currently making efforts in realizing the concept of DFFT.

DFFT is an initiative to further promote the free flow of data and enhance trust among consumers and businesses while addressing issues such as privacy, data protection, intellectual property rights and security. In other words, it is a concept that emphasizes the synergy between "trust" and "free flow of data".

To elaborate this concept, it is important for us to collaborate with other countries around the world which share the same basic values and principles regarding data, and discuss an appropriate framework for data protection through various forums and promote developing a set of rules involving many more countries.

«Approaches to promote DFFT»

In an effort to realize DFFT, the Japanese government adopted "Comprehensive Data Strategy" in December 2020, as one of the guiding principles for the promotion of DFFT in the PPC Japan.

Following this guiding principle, the PPC Japan has taken 3 concrete approaches to promote DFFT.

The first is to promote bilateral or trilateral data flow while using the existing legal frameworks for personal information protection. Japan has been so far engaged in the discussions with both the US and EU policy makers to establish a sort of symbolic framework that would allow smooth transfer of personal data among Japan, the US, and the EU, based on the nourished cooperative relationship.

The second is to introduce a global corporate certificate system. Even though the discussion has not been so matured that we can consider a specific mechanism at this point, it is one of the essential elements to materialize a worldwide trusted data free flow.

The third is to deepen discussions on the emerging risks to personal information protection at international forums. I'll discuss this in the next section.

To further stimulate the discussions stated above, we organized an online seminar at CEATEC2020. This seminar provided for the good opportunity to recognize the importance of establishing an international framework for promoting the transfer of personal data through cooperation among Japan, the US, and the EU.

«Leading discussions at the international forum»

In today's society, we are very much concerned about a trend towards digital protectionism through data localization. Unlimited government access, which could lead to an excessive state surveillance, is also a great concern for us. These two issues —data localization and unlimited government access— may hinder the trusted free flow of data. Addressing them would lead to promotion of DFFT.

It is suitable to discuss at international forums those emerging risks to personal data protection because they are global issues. Therefore, the PPC Japan has led the discussion at the OECD meeting in November 2019, proposing that those emerging risks should be discussed among the OECD members in the process of reviewing the OECD Privacy Guidelines.

It is worthwhile to note that 8 basic principles of the OECD Privacy Guidelines are still being referred to as a global standard today. Our expectation was that the Guidelines could be evolved into a new global standard that can address those risks through the review process. The review process itself was completed in April this year (2021) with the adoption of the report of the review. The discussions on government access are still going on.

«Ending remark»

In the rapidly changing global environment on digital data, it is getting more crucial to further develop cooperation with DPAs around the world.

I have no doubt that the GPA, which has been leading the global debate on privacy for over 40 years, is one of the key players in promotion of DFFT.

The PPC Japan will continue to contribute to the discussions and activities of the GPA by sharing best practices.

Debido a un rápido aumento en el uso de datos en el mundo, aunado a la pandemia de COVID-19, el entorno que rodea a los datos digitales ha estado cambiando dinámicamente. Los sistemas legales relacionados con el flujo de datos difieren de un país a otro por lo que la coordinación de políticas a través de las fronteras es esencial para el libre flujo de datos.

Japón abogó por la idea de Data Free Flow with Trust (DFFT), y actualmente se esfuerza por hacer realidad este concepto. DFFT es una iniciativa para promover aún más el libre flujo de datos y mejorar la confianza entre los consumidores y las empresas al mismo tiempo que aborda cuestiones como la privacidad, la protección de datos, los derechos de propiedad intelectual y la seguridad. En otras palabras, es un concepto que enfatiza la sinergia entre "confianza" y "libre flujo de datos".

Para continuar desarrollando este concepto, es importante para nosotros colaborar con otros países del mundo que compartan los mismos valores y principios básicos, discutir un marco apropiado para la protección de datos a través de varios foros, y promover el desarrollo de un conjunto de reglas que involucren a más países.

No tengo ninguna duda de que la GPA, que ha liderado el debate mundial sobre privacidad durante más de 40 años, es uno de los actores clave en la promoción del DFFT.

Bruno Gencarelli

Deputy to the Director for Fundamentals Rights and Rule of Law

Head of the International Data Flows and Protection Unit at the European Commission, the executive arm of the European Union.

International data flows are now part of almost any discussion on privacy, whether the focus is on stressing their critical importance in our interconnected world or addressing the challenges around ensuring that the protection travels with the data.

The present remarks focus on three developments that we are observing in our work at the European Commission, and that we believe offer new opportunities in this area.

First, the conversation around data flows has clearly become a more global and diverse one, even compared to only a few years ago. This is true from a geographical point of view: what used to be seen mainly as a transatlantic issue now involves many other regions around the globe. Today, Latin America, the Asia-Pacific area and increasingly Africa are amongst the most vibrant privacy laboratories in the world, in terms of policy initiatives, new legislations and innovative approaches. There is also more diversity with respect to the actors involved —new players are now contributing to, and often shaping, what used to be considered essentially a State-to-State matter—. International organisations but also regional networks of data protection authorities play a greater role in fostering a common understanding of these issues, promoting regulatory convergence and, in some cases, developing new transfer mechanisms. Similarly, the influence of civil society —through awareness-raising and advocacy but also collective action and litigation— as well as of the private sector —through best practices, industry standards etc.— has grown in importance also in this area of privacy.

More diversity, finally, from a substantive point of view as regards the issues at stake. This concerns, in particular, questions around the conditions under which government can access data for various public interest reasons, such as law enforcement or national security. Ensuring continuity of protection throughout the life cycle of the data —including when data needs to be accessed by public authorities— has become an area of concern for many privacy frameworks and an important consideration for the application of their rules on international transfers, requiring a delicate balancing act between different rights and interests. It has also increasingly emerged as a key component of the dividing line between democracies, that share common values and similar safeguards, and other regimes that allow abusive forms of access not in line human rights standards. The Data Free Flow with Trust initiative, launched by Japan, probably represents the best illustration of the importance of this element of the data flow landscape. Not only because, in that concept, the word "trust" refers primarily to trust in how government handles data, but also in light of the tangible developments resulting from this initiative. This includes, for the first time

ever at international level, ongoing work at the OECD on a set of common principles on trusted government access as a concrete contribution to facilitate data transfers.

This increased diversity has certainly resulted in a more complex conversation around data flows – but also a more interesting one that offers a broader range of solutions.

This brings us to a second trend: the multilateralization of cooperation on data transfers. Such an evolution does not mean that the more traditional, bilateral approach has lost importance: in the EU, for instance, two years after having created with Japan the world's largest area of free and safe data flows, we have recently concluded similar adequacy arrangements with Korea and the UK, reached an agreement in principle with the US on a successor arrangement to the Privacy Shield and expect in the coming months and years to adopt new adequacy findings, in particular with partners in Asia and Latin America. What this trend signals are rather than the bilateral approach is not the only one, as especially regional organizations and networks have emerged as important and very useful actors in this area. Model clauses as a tool for transfers provide a very good example of the unique benefits of such type of cooperation. In the past months, both the Association of Southeast Asian Nations (ASEAN) and the Ibero-American Network of data protection authorities have adopted sets of model clause for data transfers. These have the potential of significantly facilitating transfers both within those regions and between those regions and the rest of the world, as both sets are based on principles and safeguards that are shared by many jurisdictions (including the EU's recently modernized SCCs). This is also, why the European Commission is working with these two organizations to build bridges between our respective sets of model clauses, to further facilitate transfers while strengthening continuity of protection. Another example of this "network effect" is the recognition by many countries —from Colombia to Israel or Switzerland, just to mention a few examples— of EU adequacy findings as relevant also to fulfil their own international transfer requirements. This means that when a country benefits from a Commission's adequacy decision, it enjoys free flow of data not only with the 27 members of the EU but also with a dozen of other countries around the world.

Third and lastly, it is time to step up enforcement cooperation. It is somewhat surprising that, compared to other areas such as competition or financial supervision, privacy enforcers still lack to a large extent effective tools to exchange information on specific cases, provide mutual assistance, carry out joint investigations etc. when they are very often addressing similar compliance issues that moreover may simultaneously affect large numbers of consumers in several jurisdictions (such as, for example following a data breach). This is why we welcome the work of global fora, such as the GPA, and regional networks of data protection authorities to develop such tools "on the ground". At the European Commission, we intend to play our part by engaging in the negotiation of enforcement cooperation agreements with international partners.

These few examples show how much work we can and we should do together, as a global privacy community, to address challenges and seize opportunities that are increasingly global in their nature and scope.

Los flujos de datos internacionales son parte de casi cualquier discusión sobre privacidad, ya sea que el enfoque esté en enfatizar su importancia crítica en nuestro mundo interconectado o en abordar los desafíos para garantizar que la protección viaje con los datos.

Las siguientes observaciones derivan del trabajo que venimos observando en la Comisión Europea, y que creemos que ofrecen nuevas oportunidades en esta área.

Primero, la conversación sobre los flujos de datos claramente se ha vuelto más global y diversa; Esta diversidad sin duda ha resultado en una conversación más compleja sobre los flujos de datos, pero también más interesante que ofrece una amplia gama de soluciones.

En segundo lugar, existe una multilateralización de la cooperación en materia de transferencias de datos, lo que indica esta tendencia es que el enfoque bilateral no es el único. Y en tercer lugar, es que es hora de intensificar la cooperación en materia de cumplimiento, por eso acogemos el trabajo de los foros mundiales, como la GPA, y las redes regionales de autoridades de protección de datos para desarrollar dichas herramientas "sobre el terreno".

Estos pocos ejemplos muestran cuánto trabajo podemos y debemos hacer juntos, como una comunidad de privacidad global, para abordar los desafíos y aprovechar las oportunidades que son cada vez más globales en su naturaleza y alcance.

Digital economy: Scope and limits to artificial intelligence and the Internet of Things

Josefina Roman's introduction to Marc Rotenberg

Josefina Roman Vergara

INAI Commissioner, Mexico Host Coordinating Commissioner GPA 2021 @JosefinaRomanV

Artificial Intelligence (AI) techniques are being deployed increasingly, and new challenges are emerging for democratic values and fundamental rights. International organizations and national governments have established new policy frameworks to respond to such challenges. Yet, the basic principles of "fairness, accountability, and transparency" of these policy frameworks are only familiar to those engaged in data protection issues.

The keynote speech by Marc Rotenberg focused on analyzing the unique responsibilities of Data Protection Authorities in the field of AI policies, based on a global study of AI policies and practices in 30 countries. This is crucial when artificial intelligence is becoming ubiquitous and increasingly influencing our lives.

In this regard, he also exposes the relationship between AI policies and democratic values and how public officials must establish a solid data protection foundation to ensure the development of trustworthy and human-centric AI. It is also pointed out that the alternative will consist of a world of "inverted responsibility," in which machines will inexplicably make "black box" decisions about people without accountability and human control.

Resembling to the central theme of this year's Assembly- human center approach-, it is important to remember that technology should not use people; people should use it for their benefit. The changes artificial intelligence is causing in various spheres of human life invite us to reflect on the need to incorporate ethical responsibility criteria in technological practice. Despite all the deficiencies and dissatisfactions with how politics is currently carried out, it does not seem that we have found a functional substitute for this task, which ultimately refers to a collective decision about the common issues that concern us.

In modern societies, it is necessary to discuss how AI can serve to maintain and strengthen the rule of law, democracy, and human rights. However, there are also many important issues to consider, such as:

What measures should Data Protection Authorities take to face the growing challenges of AI and the Internet of Things? How important are Algorithm Impact Assessments? What is the relationship between Europe's General Data Protection Regulation and AI policy instruments?

What new challenges does AI presents that are not adequately contemplated in data protection legislation? What challenges are most urgent and should be prioritized by privacy agencies?

Actualmente, las técnicas de Inteligencia Artificial (IA) se despliegan cada vez más y surgen nuevos retos para los valores democráticos y los derechos fundamentales. Las organizaciones internacionales y los gobiernos nacionales han establecido nuevos marcos políticos para responder a tales desafíos, sin embargo, los principios básicos de "*equidad, responsabilidad y transparencia*" solamente resultan familiares para quienes se dedican a los temas relativos a la protección de datos.

Por lo anterior, la conferencia magistral impartida por Marc Rotenberg, se centró en analizar las responsabilidades únicas de las Autoridades de Protección de Datos en el ámbito de las políticas de IA, tomando como base un estudio global de las políticas y prácticas de IA en 30 países. Esto es crucial en un momento en que la inteligencia artificial se está volviendo omnipresente e influye cada vez más en nuestras vidas.

En este sentido, se deberá entender la relación entre las políticas de IA y los valores democráticos, y cómo los funcionarios públicos deberán establecer una base sólida para la protección de datos a fin de garantizar el desarrollo de una IA confiable y centrada en el ser humano.

Marc Rotenberg

President and Founder of the Center for AI and Digital Policy.
rotenberg@caidp.org

***The complete text appears in the European Data Protection Law Review, Volume 7 (2021), Issue 4, 496 - 501, https://edpl.lexxion.eu/article/EDPL/2021/4/6.:**

In the book *Computer Power and Human Reason*, the MIT computer scientist Joseph Weizenbaum wrote that we should never allow computers to make important decisions because computers will always lack human qualities, such as compassion and wisdom. Yet we find ourselves today surrounded by machines that make life-altering decisions about all of us. They decide if we get an interview for a job, if we may cross a national border, if we receive public benefits, if our children are granted admission to university, even if we are to go to jail or to maintain our freedom.

The outcomes of these decisions are not simply the concerns of the experts or the academics. There are the day-to-day lived experiences of our friends, our neighbors, and our family members in this data driven, digital economy. Many are resigned to this world. Others are not. But Weizenbaum was hardly alone in the early days of computing to recognize the risks of Artificial Intelligence. In fact, by the time he published the book many democratic governments had established comprehensive legal frameworks to regulate the processing of personal data. Here in the United States, we enacted the Privacy Act of 1974, a foundational law that set out the essential framework of modern data protection.

The central goals of 'fairness, accountability, and transparency' were well understood and established in law, as was the need for effective remedies and ongoing oversight. The framers of the Privacy Act also made clear that statistical data should be widely available if it does not pose a risk to the rights of an identifiable individual.

And here I must make two further points about modern privacy law.

First, data protection is, at its core, about fairness, it is about justice, it is about how we treat each other regardless of what a computer decides. The 'notice and choice' paradigm is an artificial construct, an effort to turn a fundamental right into a market commodity, and to provide liability immunity to those who obtain personal data. 'No- tice and choice' purposefully ignores the fact that most of the data collection occurs without participation, consensual or otherwise, of the individual.

My second point is that the real 'paradox of privacy' is that privacy requires transparency. That was understood by the drafters of the Privacy Act almost fifty years ago. That is the reason that individuals have the right to know all the information about them, and the logic and factors, that contribute to decisions about them. And modern privacy law has always recognized transparency as the most effective technique for over- sight and accountability.

When we launched the new Center for AI and Digital Policy, we took as our mission to understand the relationship between Artificial Intelligence and Democratic Values. Much as privacy advocates a generation ago explored the relationship between 'privacy and human rights' or 'cryptography and liberty,' we aimed to bridge two large conceptual categories.

The focus on democratic values is purposeful. We can easily see two AI futures —one that favors pluralistic societies and respects human dignity, another that aggregates personal data and centralizes control—.

In the first, AI offers insight into challenges such as the development of effective vaccines, the response to climate change, and the reduction of bias in criminal sentencing. AI helps fuel innovation and progress even as it subject to the regulations that builds trust and public confidence. AI remains accountable. This is the human-centric outcome.

But there is a different future, driven by the machine's desire for personal data and the desire of governments to maintain power and suppress dissent. This future conceals decisions in layers of opacity that even those in charge may not fully understand. In such a world proponents will hold out impressive results – such as a reduction in crime -- to justify

further deployment. But they will also reject independent evaluations, claiming perhaps that it is not even possible to replicate results. They will conflate correlation with causation. That is the AI-centric outcome

Of course, it is fine to prefer democratic governance over authoritarian rule but how precisely do we judge whether AI systems favor one outcome or the other?

To answer this question, we at the Center for AI and Digital Policy developed 12 metrics to assess AI. And in 2020 we published the first comprehensive review of the AI policies and practices in 30 countries. The report ***Artificial Intelligence and Democratic Values*** provides a basis to compare countries and to follow countries over time to assess whether they are making progress toward democratic values. We have engaged policymakers and urged the development of policies that safeguard democratic values.

– This week we asked the United States Office of Management and Budget to begin a public rulemaking on the use of AI by federal agencies. These regulations are re- quired by law and are now overdue. As we explained, 'Further delay by the OMB places at risk fundamental rights, public safety, and commitments that the United States has made to establish trustworthy AI.'

– Next week, we will urge the G20 countries to address the challenge of bias in AI. Earlier this year, the G7 leaders rightly called out algorithmic bias. They said they would 'take bold action to build more transparency in technologies.' We would like to see the G20 leaders take similar steps to eradicate algorithmic bias at the Summit later this month in Rome.

– And we will stand with our civil society friends in the EU and elsewhere on the need for a prohibition on remote biometric identification. *Our review of country AI practices found that the clearest distinction between AI systems in authoritarian countries and AI systems in democratic countries is the use of facial recognition for mass surveillance*. Such indiscriminate ongoing surveillance is intended precisely to coerce social behavior and limit freedom and dissent. This AI technique has been used against political protesters and religious minorities and will almost certainly be more widely deployed unless a clear prohibition is established.

Perhaps it is too familiar in the data protection world to discuss a new technology, outline its risks to fundamental rights and public safety, and then assess its compliance with legal norms. But that is not my purpose today. With AI we may indeed begin to find solutions to the pandemic, to global climate change, to the management of power grids, to the disparities in our societies that drive people apart. Instead of embedding racial bias in systems of automated decision-making, data analytic techniques should make it possible to unpack bad models, and end practices that replicate bias.

If we are to have a human-centric AI, then humans must remain in control of AI, and we must remain in control of our personal data. The UN High Commissioner for Human Rights Michelle Bachelet has stated the case directly. She has called data privacy 'an essential prerequisite' for the protection of human rights in the context of AI. And she has urged a ban on AI applications that cannot be operated in compliance with international human rights law.

We have two futures ahead. Let us choose the one in which our technologies reflect our values.

En el libro "El poder de las computadoras y la razón humana" de Joseph Weizenbaum se señala que nunca debemos dejar que las computadoras hagan las decisiones importantes porque ellas nunca tendrán las cualidades humanas de la compasión y la sabiduría. Aun así, estamos rodeados de máquinas que pueden decidir sobre nuestras vidas y alterarlas.

El enfoque en los valores democráticos tiene un propósito. Podemos ver fácilmente dos futuros de la Inteligencia Artificial: uno que favorece sociedades pluralistas y respeta la dignidad humana, y otro que agrega datos personales y centraliza el control.

Me gustaría hacer dos precisiones al respecto. Primero, las leyes modernas en datos personales y privacidad deben sobrepasar lo que las computadoras decidan; y segundo, la privacidad requiere transparencia para así encontrar un balance entre la Inteligencia Artificial y los Valores Democráticos que atañen la libertad individual.

Si vamos a tener una IA centrada en el ser humano, entonces los humanos deben mantener el control de la IA y debemos mantener el control de nuestros datos personales. Tenemos dos futuros por delante. Elijamos aquella en la que nuestras tecnologías reflejen nuestros valores.

Normative convergence to the establishment of international standards for the effective protection of a human right

Francisco Javier Acuña's introduction to Elizabeth Denham

Francisco Javier Acuña Llamas
INAI Commissioner, Mexico
Host Coordinating Commissioner GPA 2021
@f_javier_acuna

Regulatory frameworks related to advanced technologies and data governance must have standard bases to generate coherence and regulatory simplification while promoting innovation. The openness to collaboration and expanding jurisdictional horizons are essential to achieving a more homogeneous privacy and data protection framework. We cannot forget that the right to privacy is an internationally recognized human right and must be guaranteed worldwide.

At the INAI, we recognize the need to continue working in a coordinated manner on the development of international standards that contemplate the accelerated digitization process to allow the development of cutting-edge technological solutions that benefit society and, simultaneously, guarantee the protection of personal data and privacy.

Public policies must speak a common language of personal data that allows the adoption of similar principles and provisions in all regions. The mandatory nature of personal data protection must be guaranteed beyond the borders between countries through treaties or agreements between regulatory authorities.

Proposals establishing regulatory frameworks to guarantee users' privacy in the digital environment have multiplied exponentially. The year 2018 marked a turning point with the entry into force of the General Data Protection Regulation (GDPR) in the European Union and with the interference of this model in other jurisdictions. As was the case in California,

which also passed the Consumer Privacy Act (CCPA), becoming one of the most comprehensive regulations in this area in the United States.

2022 may be a year of inflection to move towards a convergence of political and regulatory frameworks. We have before us an opportunity that we cannot miss. The renewed drive for international cooperation and the opening of spaces for reflection and collaboration represents a unique opportunity to look to the future and include the adequate protection of privacy and data in the debate.

With great affection, I give the floor to Ms. Elizabeth Denham, Chair of the Global Privacy Assembly 2021.

Los marcos regulatorios relacionados con tecnologías avanzadas y gobernanza de datos deben contar con bases comunes para generar coherencia y simplificación normativa, a la vez que deben promover la innovación y la protección de la privacidad. La apertura a la colaboración y la ampliación de horizontes jurisdiccionales son fundamentales para conseguir un marco regulatorio más homogéneo. No podemos olvidar que el derecho a la privacidad es un derecho humano reconocido internacionalmente y, por tanto, debe garantizarse en todo el mundo.

En el INAI reconocemos la necesidad de continuar trabajando de manera coordinada en la elaboración de estándares internacionales. Tenemos ante nosotros una oportunidad que no podemos perder. El impulso renovado por la cooperación internacional y la apertura de espacios de reflexión y colaboración suponen una oportunidad única para mirar hacia el futuro e incluir la protección efectiva de la privacidad y los datos en el debate y en la acción.

Con un gran cariño le cedo la palabra a la Sra. Elizabeth Denham, Presidenta de la Asamblea Global de Privacidad 2021.

Elizabeth Denham

UK Information Commissioner and outgoing Chair of the Global Privacy Assembly

Solving the billion-dollar question: How do we build on the foundations of convergence?

First, why convergence has a role to play:

Our digital world is international. Data flows around the world in a heartbeat.

But the checks and balances on data are domestic. That brings problems.

It can mean that when a multinational company doesn't follow the rules, or when there is an international data breach, the ability for regulators to work together across jurisdictions can be limited, as we try to match up our differing legal systems and approaches.

It can mean that businesses have to follow several sets of rules to reach a single customer base, spread across jurisdictions. Or that people are unsure what their protections are, or where to turn for help.

And it can mean a system for international data flows based on assessments of how other nations' laws measure up to our own, no matter how many flaws we may be willing to acknowledge in our own systems.

The result is an international problem that could be costing economies around the world billions of dollars.

Convergence – through common standards and better architecture between our laws, could reduce those problems. But how do we achieve that? That is what I want to discuss today.

Building on the foundations of convergence

Let's begin with the first site of Mexico in my presentation today, the Pyramid of the Sun at Teotihuacan. A step pyramid built around 1,800 years ago, it is 75 metres high and more than 200 metres across.

It was built from two and half million tonnes of stone and earth, with each tier rested securely on the wider tier below.

This is how our moves towards greater international convergence must be constructed, if we are to reach the heights we aspire to. We must build on the carefully constructed work already completed.

The GPA has been central to the work in this area. The Assembly exists to bring together data protection and privacy authorities from around the world, and that international collaboration is the very first foundation of any convergence. What's more, work by a GPA working group to analyse ten global frameworks from across the world showed strong commonalities. In particular, there were overlaps in the core principles and data subject rights, and also in requirements for independent supervisory bodies.

Those findings should perhaps come as no surprise. The development of data protection legislation in the last decade has seen a model of building 'best of breed' laws, with the newest privacy laws, such as those in Brazil and California, standing firmly on the shoulders of other existing laws.

That's a sensible approach, as common features across laws bring a greater ability to share expertise and even work together on investigations, as well as increasing the potential for free flow of data between countries.

That free flow of data was a central motivation for the recent meeting of G7 data protection and privacy authorities, another part of the pyramid we can build upon. The meeting grew from the ambition of 'data free flows with trust', a central part of the 2019 G20 in Japan. We discussed at our G7 meeting how we could better work together on topics like AI, cookies, and national security. The focus was on where we could commit to making progress that would have a positive impact for each of us domestically.

It is clear that we have a considerably wide base with which to build further convergence. I've not touched on the Council for Europe's work in this area, for instance. But it is clear too that our work only goes so far. There are no easy answers here —if there were, we would already have taken them—.

I'll move now to my next historic sight of Mexico, and the UNESCO protected Cozumel reef which is part of the second largest system in the world, which is home to more than a thousand marine species, living side by side.

That respect for one another's cultures and approaches is another key foundation for convergence.

Convergence has to be a meeting in the middle, and I think there's a much better appreciation of that now. Our countries all have different legal structures, different administrative setups, and different cultures built on different histories.

Convergence must not mean leaving those differences behind. Instead, it needs to be about finding ways to join together these differences, and to weave a meaningful safety net of protections that work globally.

The Global Privacy Assembly really does bring voices together from all parts of the world. That diversity gives us so much collective wisdom.

Our response to the pandemic

Which brings me on to the third foundation of convergence.

The next image is the Hospital de Jesus Nazareno in Mexico City. It is said to be the oldest hospital on the continent, and to have been built at the behest of controversial Spanish Conquistador Hernán Cortés.

It remains in operation today, and like most hospitals around the world, has spent the past couple of years facing the challenges of the COVID-19 pandemic.

The pandemic has brought a great number of challenges to our community.

But it has shown the value of privacy too, and how we benefit from our shared expertise.

When the UK government wanted to develop a contact tracing app, it considered data protection at an early stage, and it consulted with my office. The government understood that answering the questions we posed on transparency, legality and fairness would help to develop an app trusted by more people.

The advice my office provided government was informed by conversations we had with colleagues across the Global Privacy Assembly network. Regulators across the world were facing similar challenges, and we all benefited from the shared wisdom of the Assembly.

Crucially —and this goes back to my conference opening yesterday—, I saw our community asking the right questions. Do we understand how people feel? And how can we make sure our input is providing practical value?

When I look now through the ICO's and GPA's work here, I think the benefits of focusing on those two questions shines through. Privacy remained relevant.

I believe the success of our community's response to COVID-19 was built on the modernisation of the GPA.

We are now a year-round assembly, able to respond quickly to challenges that arise between conferences, such as the COVID-19.

We are more collaborative than ever, able to share our expertise and to speak with one voice, as we did when we emphasised the importance of continued protections for people's data rights during the pandemic.

And we are more outward facing than ever before, working with so many of you, including the likes of the OECD, the UN, and the WHO, to make sure the advice we offered through the pandemic is rooted in practical benefit.

Our teamwork, across the privacy community, showed that we can work together, no matter our differing laws and cultures.

The pandemic showed how convergence could work.

But it showed too that we still have further to travel, if we are to truly benefit from the potential of convergence.

I will now set out the three areas where our experience shows that more must be done, to build on the foundations of convergence already in place.

The Kukulcán is a step pyramid in the south of Mexico. Across its four sides, the pyramid has a total of 365 steps, one for each day of the Mayan year.

Early separation of the year into formal calendars gave a framework for Mayan society, and was important for trade, agriculture, and religion.

As we look to the next stage of international convergence, we need to find our own framework. We need recognisable common principles that can translate across borders.

Aspects like transparency and fairness are not specific to a single law or regulatory approach, and so can act as a bridge to better international collaboration and cooperation.

This is work that is already underway within the GPA. Our Global Frameworks and Standards Working Group has focused this year on key principles that members can agree on, touching on aspects including the independence of data protection authority, international transfer mechanisms and government access to data.

The Council of Europe's work around C108 and C108+ has also looked to set common principles. And there is potential too for further exploration of how codes and certifications, including those led by business and trade groups, could assist in this area.

But it is clear that there is room for further progress.

Let's move to our next sight of Mexico.

The Copper Canyon is a network of canyons covering 65,000 square kilometers. The Canyons are linked by the Chihuahua al Pacífico, a railway passing over 37 bridges and through 86 tunnels.

The architecture needed to join the different canyons is a neat analogy for the second area where we need to build on the foundations for convergence.

It is accepted that the flow of data, from individual to organisation, from organisation to organisation, from country to country, is integral to digital innovation.

It is accepted – I hope – that such data flows rely on the public trust earned through sensible data protection regulation.

And yet we continue to consider those protections domestically.

We do have systems to transfer data internationally, of course. CBPRs enable data flows in parts of the world, while elsewhere adequacy agreements have their place.

But it remains the case that we are working with a series of bridges, rather than a single railroad.

What we need is better architecture to join together our world, and to allow different laws to work side by side. We need a railroad through the canyons.

Which brings me to our final Mexican historic site. The Temple of San Agustin is a 16th century church. A beautiful white stone building built as a convent.

But it is also abandoned. The convent was built near a lake, and flooding in the 17th and 18th century kept washing away the friars' work. Eventually, they gave up fighting the waters, and moved away.

There is a lesson there for today. We are all proud of our domestic laws, built with good intentions. But if the waters of international digital innovation keep washing away our work, at what point do we need to move to a new approach?

It is my view that there is a real urgency to this work. The pace of acceleration in digital uptake, and the increasing use of data in innovation brings those flood waters ever closer.

We are not making quick enough progress in our response. Talk of convergence has, for too long, stalled around a sense of us needing to pick a favoured legislative approach or scheme, and insist it is extended to all four corners of the world. As our community spends time focusing on faults with one another's regime, businesses are left with unwieldy processes that increasingly make privacy and data protection feel like too heavy a burden.

To put is simply, we risk all of our good work being washed away.

It is my own view that fresh thinking is needed to generate a united understanding: the old system had failed, and a new one, built on international cooperation. **What is needed is a Bretton Woods for data, repeating the 1944 conference that brought together 730 delegates from almost 50 countries to consider how the world could rebuild from war.**

A Bretton Woods conference could provide the melting pot of ideas needed to take this forward.

That could be in the shape of a global data protection accord. An accord that found common ground between nation's data protection regimes would enable member nations to better work together, and could allow for the transfer of low risk data to countries who were fellow members.

But that's only one idea —we need more ideas, and more discussion—.

I know the data protection community stands ready to be part of the solution. I see that in my work with the GPA and G7.

But that challenge must now go further.

The challenge must go to governments and international organisations with the convening power to make a Bretton Woods conference for data happen.

And then the challenge must go further afield. Data is such a broad, cross societal issue that impacts every facet of our lives. And so, the solutions must come from the bright minds across society.

Conclusion

My view is that finding a solution here —building on our existing foundations, and finding a way for international convergence— is achievable. We can make this happen.

But we must decide to do this. As a community, regulators, business, civil society, and especially policy makers, must commit to making it happen.

That will mean compromise, conversation and accepting that there is not a perfect solution.

If we get it right, there is no limit to how high we can build our pyramid.

¿Por qué hablar de convergencia?

Nuestro mundo digital es internacional. Los datos fluyen por todo el mundo en un abrir y cerrar de ojos. Pero los controles y equilibrios sobre los datos son domésticos. El resultado es un problema internacional que podría estar costando miles de millones de dólares a las economías de todo el mundo.

La convergencia: a través de estándares comunes y una mejor arquitectura entre nuestras leyes, podría reducir esos problemas. Pero, ¿cómo logramos eso? La convergencia tiene que ser un punto medio. Todos nuestros países tienen diferentes estructuras legales, diferentes configuraciones administrativas y diferentes culturas basadas en diferentes historias. La convergencia no debe significar dejar atrás esas diferencias. Al contrario, debe tratarse de encontrar formas de unir estas diferencias y tejer una red de seguridad significativa de protecciones que funcionen a nivel mundial. Necesitamos principios comunes que puedan atravesar las fronteras.

Mi opinión es que encontrar una solución construyendo sobre nuestros cimientos existentes y encontrando un camino para la convergencia internacional, es factible.

Como comunidad, las autoridades reguladoras, las empresas, la sociedad civil y especialmente los formuladores de políticas deben comprometerse a que esto suceda.

Eso significará compromiso, conversación y aceptación de que no existe una solución perfecta.

Panels

Data Protection and Human Rights: Mass surveillance by facial recognition and analysis of metadata

Omar Seghrouchni

President of the CNDP of Morocco (Commission Nationale de contrôle de la protection des Données à caractère Personnel)

The maintaining of balance of the equation freedom-surveillance is one of the main demanding challenges in the actual digital context. Moreover, building and ensuring a strong democracy entails the right harmony and homogeneity between personal data protection and traceability.

Nowadays, biometric technologies are becoming more and more abundant and precise. The digitalization of society is turning us, each and every citizen, into a producer of traces and personal data.

The accepted level of traceability depends on the level of respect for the privacy of others and the democratic values of the society we live in. As such, consent is a central element for the personal data processing of the citizen.

Whereas fingerprint collection requires the physical presence of the data subject, iris scanning also requires the physical presence of that data subject.

Although, facial recognition can be carried out without the knowledge of the citizen, who therefore finds himself traced without his prior consent. Consequently, facial recognition regulation must be improved so that the decisions induced by it should consider recourse, transparency, explicability, and loyalty of algorithms.

As part of its mission to protect individuals regarding their personal data processing, the CNDP of Morocco had launched, in 2019, a moratorium on facial recognition. The aim was to regulate the purposes for which facial recognition can be used and to prevent any potential misuse of the personal data processed through it. Therefore, it is in our interest not to treat technologies in a fragmented and scattered way, but rather to have a broad

and macro vision regarding the bricks of trust; and one of these bricks of trust is the notion of identification.

Moreover, the SDG (Sustainable Development Goal) 16.9 calls for every citizen to have a legal identity by the year 2030.

The availability of several public sectoral digital identities, which can be cross-referenced and interconnected through a single regal identity, will strengthen privacy protection without forgetting that nowadays, mass surveillance doesn't involve States only, but also commercial and private structures.

It is by reflecting and working on concrete cases with the various actors concerned that it will be possible to build, together, a framework that makes sense, both operationally and in terms of compliance with personal data protection.

Therefore, we believe that it is important to work at the international level towards a universal identity framework, in accordance with the democratic values of the modern world.

At last, there is only one evidence in terms of this subject: **"***To live digital, one should breathe personal data protection*".

Mantener el equilibrio entre la libertad y la vigilancia es uno de los principales desafíos en el contexto digital. Hoy en día, las tecnologías biométricas son cada vez más abundantes y precisas. La digitalización de la sociedad nos está convirtiendo, a todos y cada uno de los ciudadanos, en productores de huellas digitales y datos personales. El nivel de trazabilidad aceptado depende del nivel de respeto por la privacidad de los demás y los valores democráticos de la sociedad en la que vivimos.

Como parte de la misión de proteger a las personas con respecto al procesamiento de sus datos personales, la CNDP de Marruecos lanzó, en 2019, una moratoria sobre el reconocimiento facial, con el objetivo de regular los fines para los que se puede utilizar esta tecnología y prevenir cualquier posible uso indebido de los datos personales procesados a través de ella.

Creemos que es importante trabajar a nivel internacional hacia un marco de identidad universal, de acuerdo con los valores democráticos del mundo moderno.

Ann Cavoukian, Ph.D., LL.D. (Hon.), M.S.M.
Executive Director, Global Privacy & Security by Design Centre

The Essential Need for Privacy by Design to Preserve our Privacy,

Well Into the Future

Privacy is essential: it forms the foundation of our freedom and must be preserved at all cost, now, and well into the future. With surveillance mounting, we must be proactive in our privacy-protective measures, in an effort to prevent the harms from arising. That is what

Privacy by Design is all about: embedding privacy into your operations —baking it into your code—, so that privacy invasive efforts can be prevented, right from the outset! Learn all about the 7 Foundational Principles of PbD and start protecting privacy, right from the outset!

Privacy forms the foundation of our freedom —you cannot have free and open societies without a solid foundation of privacy—. Privacy is a necessary condition for societal prosperity and well-being. Innovation, creativity and the resulting prosperity of a society requires freedom, and privacy forms the essence of our freedom.

Privacy equals control - personal control on the part of the data subject relating to the use and disclosure of one's personal information. User control is critical to preserving freedom of choice and personal freedom, the essence of privacy! Without privacy, Individual human rights, property rights and civil liberties —the conceptual engines of innovation and creativity—, could not exist in any meaningful manner. And context is key: only the individual knows the context associated with a given situation well enough to determine its sensitivity, or lack thereof, and the need for privacy. This remains highly personal, requiring the individual involved to make such determinations.

The Germans created an excellent term to capture the essence of this view: "Informational self-determination". It must be the individual who determines the fate of his or her personal information. Nowhere is this more critical than in the context of health information and electronic medical records, which by their very nature, may be accessed quietly by digital means unless strong protections are proactively embedded within, to prevent unauthorized access to by third parties. Nowhere is Privacy by Design needed more than in health-related records, where proactive measures to shield the data from unauthorized third-party access are critical.

Strong security goes hand-in-hand with privacy! While the term privacy subsumes a much broader set of protections than security alone, in this day and age of dily hacking exploits, a strong foundation of security, from end-to-end, with full lifecycle protection, is an absolute must. Privacy AND security must appear together, not the dated zero-sum, eith/or model of one interest vs the other.

Privacy by Design drives this home by requiring the need to proactively embed both privacy and security measures directly into one's operations. And since the 7 Foundational Principles of Privacy by Design are now followed all around the world, having now been translated into 40 languages, there is no reason why we cannot preserve our privacy now, and well into the future. We cannot allow surveillance to strip us of our privacy, our freedom! Say NO to surveillance, and YES to Privacy by Design! We can do this!

La privacidad es esencial pues forma la base de nuestra libertad y debe preservarse a toda costa, ahora y en el futuro. No se pueden tener sociedades prósperas, libres y abiertas sin una base sólida de privacidad.

La privacidad es igual a control: control personal por parte del interesado en relación con el uso y la divulgación de su información personal. El control del usuario es fundamental

para preservar la libertad de elección y la libertad personal. Sin privacidad, los derechos humanos, los derechos de propiedad, las libertades civiles, los motores conceptuales de la innovación y la creatividad, no podrían existir de manera significativa.

No podemos permitir que la vigilancia nos despoje de nuestra privacidad, ¡NO a la vigilancia y SÍ a la privacidad por diseño! ¡Juntos podemos hacer esto!

Brenda Leong

Partner at BNH. Previously, senior counsel and director of AI and Ethics at the Future of Privacy Forum

Facial recognition technology continues to evolve and appear in new contexts. Common existing services include: (1) safety and security; (2) access and authentication; (3) photograph and video storage and organization; (4) accessibility to accounts, and (5) marketing and customer service. There are also, however, growing concerns about the privacy protections needed for the responsible use of this expanding technology.

Facial recognition systems are particularly sensitive because they involve a unique part of the human body, one that is directly related to our identity and has the potential to infringe upon our concept of self in public, private, and commercial contexts. This impacts our ability to feel anonymous or obscure in public or in large crowds.

Thus, privacy discussions about the personal data generated by facial recognition systems must necessarily consider the heightened considerations for sensitive data, as well as reflect the larger debate around ubiquitous surveillance concerns. It will not always be clear to the general public who owns or operates the surveillance cameras around them, who has access to the data being generated, whether the data collected is subject to facial recognition analysis, and if so, by whom, for what purposes, or subject to what protections and controls. Both the service providers, and the enterprise platforms bear some responsibility for the social implications of how their system recommendations impact individuals.

Historically, one's image wasn't easily collected, tracked, or shared by either commercial entities or governments. But now it can be. The technical focus is on data protection and system reliability, but these are not the only concerns. There is also the potential to unfairly or illegally discriminate. For example, a retail chain might create its own dataset of "known" offenders without any clear standards for who is targeted, no practice by which they are notified or can appeal their inclusion, resulting in individuals being broadly denied service without any due process. Likewise, government misidentification can lead to innocent people on "watch lists," with increased risk of bad results for minorities and other at-risk populations.

The ethical considerations of where and how to use facial recognition systems exceed the boundaries of traditional privacy considerations. These systems are built on existing systems that reflect human biases and automate them. Having "humans in the loop" will not mitigate

this; trained programmers must test and audit systems for bias and be able to recommend corrective measures. The social impacts of this are only beginning to be understood.

There are beneficial use cases for facial recognition systems. Several companies offer tools that incorporate facial detection, characterization, and/or identification to assist the blind and low vision communities. There are screen readers that provide audio or braille user interfaces for people who are blind or have impaired vision. Additional use cases may not inherently be either good or bad. Profiling shoppers, tracking online preferences and personalizing recommendations or experiences are features some consumers may value, but others strongly oppose.

Determining whether a proposed use is compatible with consumer expectations requires considering factors such as the context of data collection; a reasonable awareness of how the data will be used; whether facial recognition is merely a feature of a product or service or integral to the service itself; and how the collection, use, or sharing of facial recognition data will likely impact the individual consumer or identified social groups.

When they were first implemented, government-issued passports were considered offensive, and the later requirement that they include a photo shocked the public consciousness. The U.S. and the United Kingdom have consistently resisted the call for a national ID card. These historical discussions reflect the ongoing need to determine the appropriate balance of technological, legal, and policy standards and protections, along with the underlying threshold question of whether some systems are simply too high risk to implement regardless of perceived benefits.

Technology has only accelerated the practice of identification and tracking of people's movements, whether by governments, commercial businesses, or some combination thereof, leading to the real concerns about an ultimate state of ubiquitous surveillance. How societies faces these challenges will determine how we move further into the conveniences of a digital world, while continuing to embrace our fundamental ideals of personal liberty and freedom.

La tecnología de reconocimiento facial continúa evolucionando y apareciendo en nuevos contextos, por eso existen crecientes preocupaciones sobre las protecciones a la privacidad necesarias para el uso responsable de las nuevas tecnologías en expansión.

No siempre estará claro para el público en general quién posee u opera las cámaras de vigilancia a su alrededor, quién tiene acceso a los datos que se generan, si los datos recopilados están sujetos a análisis de reconocimiento facial y, de ser así, por quién y con qué fines, o sujeto a qué protecciones y controles. Tanto los proveedores de servicios como las plataformas empresariales tienen cierta responsabilidad por las implicaciones sociales de cómo las recomendaciones de sus sistemas afectan a las personas.

Las consideraciones éticas de dónde y cómo usar los sistemas de reconocimiento facial superan los límites de la privacidad. Los impactos sociales de esto apenas comienzan a entenderse.

Claudia May Del Pozo

Director of C Minds' Eon Resilience Lab
LinkedIn Claudia May del Pozo

Latin America's Take and Progress on Privacy, Surveillance, and AI

The tech-related privacy and surveillance conversation takes a specific turn when looking at it from a Latin American lens, for two main reasons. The first is related to history: the region has a long record of dictatorial governments that have resorted to tools of surveillance, control, and repression, and —despite the efforts to strengthen political systems and the democratic procedures— a culture of authoritarianism that still lingers. The second has to do with the state of data and technology regulation. The region's countries urgently need to update their legal systems to prevent technological abuses: not all countries have data protection laws and most of the ones that do have not revised them to include the challenges posed by digital technologies. Only Brazil has taken this step, with its version of the European Union's General Data Protection Regulation (GDPR). The region also needs to strengthen its awareness, knowledge, and tools to ensure responsible development and adoption of pioneer tech such as artificial intelligence, without which potential Human Rights violations may lie around the corner.

As the Director at a Mexican innovation agency that seeks to promote the responsible use and development of new technologies for good in Latin America, we address this second challenge. From our research and experience, the responsible tech focus shortfall in Latin America stems from insufficient knowledge surrounding the risks that new technologies, like artificial intelligence (AI) systems, represent, a challenge that we have seen across emerging economies and higher-income countries. This difference in awareness could, in part, come down to the state of regulation.

Some of the regions with the most awareness regarding potential AI risks include the European Union and the United States. The EU Commission has proposed the EU AI Act, the first comprehensive effort to create more responsible AI systems. This law suggests companies follow certain requirements based on the risk-level of their AI system, with high-risk applications including facial recognition (FR) technology. Tech-specific efforts include San Francisco's government ban on FR technology back in 2019, which led to at least 16 other municipalities across the country to follow suit, among other bans and ordinances in the country.

Research has shown that citizens from countries like the US and in Europe, in highly monitored places, feel threatened by the amount of technology monitoring them, but, interestingly enough, this feeling is not necessarily shared by their peers in Latin America. We've spoken to citizens of Merida, a heavily surveilled city in Yucatan, Mexico, who claim they feel safer and freer since the government placed cameras around the city. A person's level of acceptance of surveillance technology may often depend on their sense of safety. For instance, a person in Latin America could be more likely than a person from the US and Europe to feel unsafe. This showcases a clear contrast in what different regions might

consider important, prioritary, or even dangerous. That is not to say that Latin America should accept the non-ethical use of new technologies if it addresses a key challenge, but rather that its views and approach to regulation might and should differ from that of the places leading the conversation regarding AI ethics, namely the US and Europe.

The good news is that many governments in the region are already looking at how to approach the matter from their own contexts and realities. Some notable examples include the AI Privacy by Design and Default Regulatory Sandbox carried out by the Colombian Superintendence of Industry and Commerce (SIC) starting in 2021. In 2022, the Colombian government adopted the ethical AI recommendations presented by UNESCO. In turn, Mexico has been working on a policy prototype for transparent and explainable AI systems, led by Meta and C Minds' Eon Resilience Lab, together with the Inter-American Development Bank (IDB) and with the support of the National Institute for Access to Public Information and Data Protection (INAI). Meta, C Minds' Eon Resilience Lab, and the IDB are also working with the E-Government and Information Society Agency (AGESIC) and the Regulatory and Personal Data Control Unit (URCDP) in Uruguay to carry out a policy prototype for privacy enhancing technologies. Most encouragingly, Brazil is in the process of approving the Brazilian AI Bill, which establishes principles, duties, and guidelines for developing and applying said technologies.

In addition to bringing the region's regulations up to speed, these approaches will also bring a much-needed broader perspective to the international conversation on pioneer tech regulation such as AI.

La tecnología que implica privacidad y vigilancia desde la perspectiva latinoamericana es muy distinta por dos razones principales.

La primera está relacionada con la historia: gobiernos dictatoriales que han recurrido a herramientas de vigilancia, control y represión y, a pesar de los esfuerzos por fortalecer los sistemas políticos democráticos, persiste una cultura de autoritarismo.

La segunda tiene que ver con el estado de regulación de datos y tecnología. Los países de la región necesitan urgentemente actualizar sus sistemas para prevenir abusos tecnológicos; no todos los países tienen leyes de protección de datos personales.

Como Directora de una agencia mexicana de innovación que busca promover el uso responsable y el desarrollo de nuevas tecnologías para el bien en América Latina, abordamos este segundo desafío.

A partir de nuestra investigación y experiencia, el déficit de enfoque tecnológico responsable en América Latina se deriva del conocimiento insuficiente sobre los riesgos que las nuevas tecnologías, como la inteligencia artificial, tienen en las personas.

Promotion of an ethical approach into organizations

Bojana Bellamy
President Centre for Information Policy Leadership

CIPL has been at the forefront of promoting accountability for many years, most notably by developing the CIPL Accountability Framework to provide concrete examples of how to implement effective, demonstrable, and enforceable accountability measures through organisations' privacy management and compliance programs. In our work, we have learned that accountability is about organisations stepping up and changing behaviour to demonstrate their commitment to data privacy. Values and ethics inform and shape how organisations put accountability into practice. Consequently, many businesses today are investing in ethics and standards, and data privacy and data ethics are increasingly becoming part of broader corporate values.

Trust, ethics, and data

In the context of accountability and ethics, it is crucial to consider trust as an aspect that drives corporate behaviours. Companies are increasingly putting trust as their leading operational principle and developing tools to measure and report on activities that promote and build trust.

Moreover, ethics are linked with legal compliance. Very often, companies have to make ethical decisions to comply with data privacy principles, such as fairness and transparency, and decide whether legitimate interest balances the rights of individuals. Businesses that employ ethical decision-making and act beyond legal compliance tend to excel in these decisions.

Another consideration related to accountability and data ethics is the efficient and accountable use of data. Data is critical for our digital ecosystem. External developments such as increasing investors' focus on environmental, social and corporate governance (ESG), privacy, and security have fostered the ethical use of data. Investors care about businesses that will maintain value and show that they are responsible. As a result, we are seeing some companies appoint chief responsibility or trust officers who focus on exploring the impact of their businesses on stakeholders and society at large.

However, we should realise that data ethics are not only about addressing the risks and harms of data used in the technologies and digital services. Data ethics can help us understand the benefits of data use and allow, in some instances, to consider the negative impact of not using or not sharing. Thus, ethical decision-making is not one-sided; it involves both risk assessment and consideration of added benefits.

New developments

In recent years, we have observed several new developments in the field of accountability and data ethics. First, the COVID-19 pandemic forced companies to make some difficult ethical decisions, namely, on how to responsibly use data in the context of the pandemic. **These difficult decisions have been addressed more efficiently, balancing business and individual interests by companies that have put in place accountability and data ethics frameworks.** This experience proves that an accountability framework within an organisation is crucial. It provides a roadmap and a compass for companies facing new challenges and can also contribute to agile and responsible data use.

Second, the increased use of AI and data analytics raises many ethical issues. In order to address these novel concerns, companies and public sector bodies will have to develop best practices, policies and procedures for developing and using accountable AI. We are already seeing some of the companies, leaders in AI, make large investments in emerging best practices and tools for responsible AI that are designed to implement ethical AI principles into practice. These include AI governance frameworks, with oversight committees, fairness and non-bias tools, privacy-preserving technologies, AI impact assessments, ongoing audits of algorithms, training of data scientists and engineers on data ethics, etc. This shift is influenced **by companies moving beyond compliance and understanding that maintaining and increasing trust in AI is the key**. Accountability and data ethics help companies to address complex problems, emerging technologies and make consistent decisions. Adherence to these frameworks will ultimately enable these organisations to unlock the potential of data, new technologies, AI and to bring benefits to society, while also positively impacting business outcomes.

Data privacy regulators should proactively encourage and incentivise the development of these best practices for responsible and ethical data use.

CIPL is determined to drive good data practices, and good data practices are based on ethical uses. This convergence between data practices and ethics is what CIPL has been promoting through its Accountability Framework and what CIPL continues to promote in conversations with business leaders and regulators.

En el contexto de la responsabilidad y la ética, es crucial considerar la confianza como un aspecto que impulsa los comportamientos corporativos, la ética que está ligada al cumplimiento legal, y el uso eficiente y responsable de los datos.

La ética de datos puede ayudarnos a comprender los beneficios del uso de datos y permitir, en algunos casos, considerar el impacto negativo de no usarlos o compartirlos.

Por lo tanto, la toma de decisiones éticas no es unilateral; implica tanto la evaluación de riesgos como la consideración de beneficios adicionales.

Las empresas tienen que tomar decisiones éticas para cumplir con los principios de privacidad de datos, como la equidad y la transparencia, y decidir si el interés legítimo equilibra los derechos de las personas. La responsabilidad y la ética de los datos ayudan a las empresas a abordar problemas complejos, tecnologías emergentes y tomar decisiones coherentes.

La CIPL está decidida a impulsar buenas prácticas de datos basados en usos éticos.

Irina Raicu

Director of the Internet Ethics program
at the Markkula Center for Applied Ethics
@IEthics

Privacy is a key ethical issue. We frequently think of it as a human right, but as others have already noted on this panel, privacy is also related to justice, fairness, and the common good.

Privacy by design considerations imply a need to listen to and to protect those who are most vulnerable —especially in the context of massive information asymmetry—. Technologists, and possibly regulators too, sometimes overlook how little most people understand about the opaque ecosystems in which they live their online lives. This discrepancy is part of what leads to unfair outcomes for people who are in no position to defend their own privacy.

The ethical lens of the common good focuses on the conditions required for a whole community to thrive; privacy is one of those conditions.

Since we're talking about various ethical lenses, we also need to acknowledge that ethical analysis is a skill, which needs to be developed and practiced; therefore, technologists and others within companies would benefit from relevant ethics training, which should address privacy as one of multiple, sometimes clashing, ethical issues.

The center where I work offers a compendium of free materials particularly relevant to this conversation, titled "Ethics in Technology Practice" One of them includes a useful analogy developed by the philosopher Shannon Vallor, who notes that ethical issues are like birds. Like birds (she writes), ethical issues are everywhere, though sometimes difficult to see; they are varied, but frequently concentrated in particular areas or contexts; they are also more likely to be "noticed by people who are in the habit of looking for them".

Vallor notes that [g]etting good at noticing and identifying ethical issues, like birdwatching, is a skill that takes repeated practice to develop… What matters is *not* a theoretical knowledge of ethics (though this can be a useful tool, like a 'birdwatchers' field guide), but *practical experience and skill* assessing the ethical landscape in those areas connected to our life and work.

These experiences and skills are increasingly in demand, and increasingly necessary among those who shape technology that helps shape all of us —including our perceptions of privacy—.

Ethical questions are very contextual, so frameworks and lists of principles can only take us so far. We need to start talking about how to operationalize those principles, and how to strengthen our ethical analysis "muscles."

In fact, relevant ethics training is best provided even before people start their professional roles: The movement now is toward requiring it as an inherent part of the education of technologists and designers. For those who didn't get such training elsewhere, however, it is important to include it in the onboarding process and as an ongoing part of work within any organization.

But technologists and designers can't do it all on their own and solely on the basis of ethics. The right incentives must also be in place. And laws can do much to create powerful incentives and disincentives.

Still, privacy as an ethical issue takes us beyond legal compliance. There will always be novel questions and gray areas in which it's not clear which laws apply, or how —and sometimes laws clash too—. So, no matter how many laws we have, people will still have to make ethical determinations about what actions to take (or not take).

Also, many privacy laws exempt, for example, small businesses below a certain threshold; but the fact that such companies don't have to worry about compliance doesn't mean they're exempt from ethical duties.

We need both ethics and law, and we need regulators who understand that. In the context of AI, for example, the technology is so powerful, and it's being deployed so quickly in so many different aspects of our lives, that regulators need to move more quickly too. They need to understand the issues and resist the hype, making sure that they have technologists on staff who can explain both the capabilities and the limitations of technology. They need to have multidisciplinary teams and to find ways to listen to the voices of those impacted.

The title of our panel was "Promotion of An Ethical Approach into Organizations". It is worth noting that "organizations" covers more than the corporate context.

Las consideraciones de privacidad por diseño implican la necesidad de escuchar y proteger a aquellos que son más vulnerables. Los tecnólogos, y posiblemente también los reguladores, a veces pasan por alto lo poco que la mayoría de la gente entiende sobre los ecosistemas opacos en los que viven sus vidas en línea. Esta discrepancia es parte de lo que conduce a resultados injustos para las personas que no están en condiciones de defender su propia privacidad.

El lente ético del bien común se enfoca en las condiciones requeridas para que toda una comunidad prospere; la privacidad es una de esas condiciones.

La privacidad como cuestión ética nos lleva más allá del cumplimiento legal. Siempre habrá preguntas novedosas y áreas grises en las que no está claro qué leyes se aplican

o cómo, y algunas veces las leyes también chocan. Por lo tanto, no importa cuántas leyes tengamos, las personas aún tendrán que tomar decisiones éticas sobre qué acciones tomar (o no tomar).

Necesitamos tanto a la ética como a la ley, y que los reguladores entiendan eso. Necesitan comprender los problemas, asegurándose de contar con tecnólogos que puedan explicar tanto las capacidades como las limitaciones de la tecnología. Necesitan tener equipos multidisciplinarios y encontrar formas de escuchar las voces de los afectados.

Stephen Bonner

Deputy Commissioner, Executive Director Regulatory Futures and Innovation Information Commissioner's Office, UK

When it comes to ethical and trustworthy approaches to personal data, legislation provides a minimum baseline. Building *genuine* trust needs something beyond the minimum.

If you go into a restaurant you expect a minimum standard of cleanliness, and that is usually laid down by the law. But what if you care about animal welfare as well? You might be more likely to go to a restaurant which advertises the use of free-range animal products. If you have concerns about the environment, you might track down businesses using organic products. You might be seeking out a commitment to fair trade or want to support local economies.

So, this isn't just about finding a place that's going to sell you food that doesn't make you ill. It's about places that operate in line with your personal values and standards, and make you feel more comfortable as a result.

The same principle could also extend to employees. If your organisation's values and standards don't align with their personal principles, they could, and often do, choose to work elsewhere. This isn't a good experience for individuals, and it's also bad for business.

The world of data protection is the same. Let's look at artificial intelligence as an example. Implementing AI into your service might have all kinds of potential benefits like improved speed and efficiency, but if people don't trust it, they won't use it – and might even avoid interacting with organisations who do.

The way to create that trust is to demonstrate you are worthy of it. People are seeing through the phenomenon of 'ethics washing' —techniques like using the 'right' language to cover for unethical practices—, oversight teams with no power, studies funded by the organisations themselves.

Going back to our example of AI, we see genuine explainability and transparency as the foundations of trustworthiness. Building trust means being able to clearly explain upfront how your system works, what personal data it uses and where that data has come from —as well as who you might be sharing it with—.

The ICO has been focusing on four key areas as part of our consultation on the role of data ethics in complying with the GDPR: existing practices, supporting organisational structures, ethical decision-making processes; and information compliance programmes.

We've also been thinking about the hugely important principle of 'fairness', which is one of the cornerstones of data protection. In particular, who should decide whether processing is deemed 'fair'? How should this be assessed?

As regulators in this world, the key questions for us are these: how does an organisation build an ongoing set of structures which do the best for the individual, attract the best staff and create the best outputs?

And most importantly – who is accountable for making sure that happens?

La implementación de IA puede tener todo tipo de beneficios potenciales, como mayor velocidad y eficiencia, pero si las personas no confían en ella, no la usarán, e incluso podrían evitar interactuar con organizaciones que sí lo hacen.

Generar confianza significa ser capaz de explicar claramente cómo funciona su sistema, qué datos personales usa y de dónde provienen esos datos, así como con quién podría estar compartiéndolos.

El ICO se ha centrado en cuatro áreas clave como parte de nuestra consulta sobre el papel de la ética de datos en el cumplimiento del GDPR: prácticas existentes, estructuras organizativas de apoyo, procesos éticos de toma de decisiones; y programas de cumplimiento de la información. Así como el principio de "equidad", que es una de las piedras angulares de la protección de datos.

Como reguladores en este mundo, las preguntas clave son: ¿cómo construye una organización un conjunto de estructuras que hacen lo mejor para el individuo, atraen al mejor personal y crean los mejores resultados? Y lo más importante: ¿quién es responsable de asegurarse de que eso suceda?

The future of privacy and technology: challenges and possible solutions

Wojciech Wiewiórowski

European Data Protection Supervisor

I always considered that privacy rules are not ends in themselves but should remain means for safeguarding and promoting human dignity and social justice, locally and globally. Means to protect the living souls of our societies.

The fight for individual rights must be a joint action, an effort made by societies as a whole. Together, we can shape a safer digital future, by making sure that data protection is embedded, by design and by default, in innovation.

But at the same time, I am not naïve about the future: we will also see a proliferation of inter-connected devices, extending the attack surface for criminal and state-sponsored hacking, to gain access to protected information and disrupt services.

We will also see more use of biometric technologies, facial and automatic recognition systems, Artificial Intelligence, Augmented/Virtual Reality, increasingly deployed in the spaces and facilities of public utility.

We are not questioning any technology per se. But, as EDPS, I will continue to oppose some untested and particularly invasive applications of certain technologies.

For instance, I will continue to call to consider a ban on online targeted advertising based on pervasive tracking.

I will also continue to call for a ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination;

Moreover, as much as we need control over data and digital sovereignty, we also need digital solidarity. Digital solidarity means making data work for all people, especially the most vulnerable. It means bringing an end to business models of constant surveillance and tracking, which have been damaging the trust in the digital society. And please remember that for me —a Polish man born in 70s— the word Solidarity has also a historical meaning of changing the world together.

We should all engage on these issues openly to have an informed debate around on how personal data can be used to serve the 'public good', whether in times of crisis, or not. The "new normal" should not give way to the permanent erosion of rights we have fought so long and hard to promote.

This is not only a discussion for lawyers, IT experts or data protection geeks but a truly "political" discussion —in the original Greek sense of the word— i.e. a discussion on how a society wants to organise the life in the City.

I am confident that we have this capacity to collectively work to make human dignity and social justice a reality for tomorrow's digital world.

Las reglas de privacidad deben seguir siendo medios para salvaguardar y promover la dignidad humana y la justicia social, a nivel local y global. La lucha por los derechos individuales debe ser una acción conjunta, y dar forma a un futuro digital seguro, donde la protección de datos esté integrada, por diseño y por defecto, en la innovación.

Así como necesitamos control sobre los datos y la soberanía digital, también necesitamos solidaridad digital. Solidaridad digital significa hacer que los datos funcionen para todas las personas, especialmente para las más vulnerables.

Todos debemos comprometernos a tener un debate informado sobre cómo se pueden usar los datos personales para servir al "bien público", ya sea en tiempos de crisis o no. La "nueva normalidad" no debe dar paso a la erosión permanente de los derechos por los que hemos luchado durante tanto tiempo y con tanto esfuerzo. Estoy convencido de que tenemos la capacidad de trabajar colectivamente para hacer de la dignidad humana y la justicia social una realidad para el mundo digital del mañana.

Panel Summary
Written by the INAI's GPA Secretariat

The panel was moderated by Wojciech Wiewiórowski, European Data Protection Supervisor, and featured the following panelists: Erin Egan, Vice President of Public Policy and Policy Privacy Officer, Facebook, Meta; Jane Horvath, Chief Privacy Officer at Apple; Keith Enright, Chief Privacy Officer Google; Damien Kieran, Chief Privacy Officer at Twitter, and Andrew Clearwater, Chief Trust Officer at One Trust.

The panel's purpose was to open the discussion to explain upcoming technology and data controllers, as well as privacy challenges and solutions. Entries were based on the themes of privacy by design and privacy by default, and responsibility and accountability as key elements to ensure proper compliance with privacy and data protection legislation.

During the session, the participants explained from their experience how they had implemented compliance programs focused on protecting personal data and privacy through adopting tools and technologies that protect privacy by design. As well as through impact assessments, feedback from users and interested sectors, experts in the field to guarantee

that personal data is treated appropriately within their organizations, and by adopting privacy training programs for all their personnel from senior management.

They also highlighted the importance of generating trust in users through the protection of personal data and guaranteeing transparency on the uses and exchange of personal data towards users as a competitive advantage, which also helps to promote the innovation of new technologies designed to protect the privacy of individuals.

El panel fue moderado por Wojciech Wiewiórowski, Supervisor Europeo de Protección de Datos y contó con la participación de los siguientes panelistas: Erin Egan, Vicepresidente de Políticas Públicas y Director de Privacidad de Políticas de Facebook; Jane Horvath, Directora de privacidad en Apple; Keith Enright, Directora de privacidad Google; Damien Kieran, Directora de Privacidad en Twitter y Andrew Clearwater, Director de confianza en One Trust.

El objetivo del panel consistió en abrir el debate para dar explicación sobre la próxima tecnología y los controladores de datos, así como en los desafíos y soluciones en materia de privacidad. Las participaciones se basaron en los temas de la privacidad por diseño y por defecto, así como en la responsabilidad y la rendición de cuentas como elementos clave para garantizar el adecuado cumplimiento de la legislación de protección de datos y privacidad.

Durante la sesión, los participantes expusieron desde su experiencia cómo han implementado programas de cumplimiento enfocados a la protección de datos personales y privacidad, mediante la adopción de herramientas y tecnologías que desde el diseño protegen la privacidad, así como por medio de evaluaciones de impacto, retroalimentación con los usuarios y sectores interesados, así como de expertos en la materia para poder garantizar que los datos personales se traten de manera adecuada al interior de sus organizaciones, adoptando desde la alta dirección programas de capacitación sobre privacidad para todo su personal.

Se destacó también, la importancia de generar confianza en los usuarios, por medio de la protección de datos personales y garantizando la transparencia sobre los usos y el intercambio de datos personales hacia los usuarios, como ventaja competitiva, que además ayuda a fomentar la innovación de nuevas tecnologías diseñadas para proteger la privacidad de las personas.

The challenge of compliance: The perspective of Data Protection Officers

John Edwards

Former Privacy Commissioner, New Zealand.
Information Commissioner, ICO UK

Information Commissioner, ICO UK

The topic for today is the challenge of compliance and the perspective of data protection offices. With massive fines, reputational risk, and brand value on the line, it takes much responsibility on the shoulders of data protection officers.

What does it take to be a successful DPO? Where should a DPO be in an organization? To whom should they report? What is the value of contracting out DPO services instead of maintaining an in-house capability? What about the challenge of locating the necessary multi-disciplinary skill set in one person? Does a DPO need to be a data scientist? An expert in AI and encryption? A lawyer qualified in all the jurisdictions the company operates in? Is it the DPO who is responsible for determining whether that new processing is a legitimate interest?

What are the challenges facing technologies that make intensive use of personal data? What obstacles must they overcome to enable the cross-border data flow between related parties? What are the challenges of adapting a data protection model to multiple jurisdictions and regulations?

Understanding data protection remains a fundamental part of any modern organization. Understanding not only what the law says but also what that means in practice and how it relates to your customers, staff, and stakeholders remains a specialist job.

DPOs are the ones who best understand what any innovation around data will mean to customers. The privacy professional is the eyes and ears of an organization in that respect. I have seen from the listening tour the amplification effect and value of various DPO networks in sharing knowledge and making efficiencies.

As a result of this, I invite you to discuss all these questions and listen to different perspectives from the private sector. Welcome to this panel.

El tema para analizar en este panel se enfoca en el reto del cumplimiento y la perspectiva de las oficinas de protección de datos y la gran responsabilidad que tienen. Para esto, surgen diversas preguntas, tales como:

¿Qué se necesita para ser un DPO exitoso? ¿Dónde debe estar un DPO en una organización? ¿A quién deben informar? ¿Un DPO necesita ser un científico de datos? ¿Cuáles son los retos a los que se enfrentan las tecnologías que hacen un uso intensivo de datos personales?

Comprender la protección de datos sigue siendo una parte fundamental de cualquier organización moderna. Comprender no solo lo que dice la ley, sino también lo que eso significa en la práctica y cómo se relaciona con sus clientes, personal y partes interesadas. Los DPO son los que mejor entienden lo que significa cualquier innovación en torno a los datos personales, pues son los ojos y los oídos de una organización en temas de privacidad.

Los invito a escuchar diferentes perspectivas del sector privado. Bienvenidos a este panel.

Anna Zeiter, LL.M., CIPM, CIPP/E

Associate General Counsel & Chief Privacy Officer eBay Inc.
LinkedIn Anna Zeiter

The challenge of compliance: The perspective of Data Protection Officers

Three major things companies need for successful Privacy and Data Protection Compliance

Privacy and Data Protection are extremely hot topics. Globally, we see that on the legislative, executive as well as on judicative front. Almost on a weekly basis new privacy and data protection regulations are being passed by legislative bodies around the globe. Besides that, Privacy and Data Protection Supervisory Authorities have become more active during the last couple of years and almost every day we can read in the media news about high fines being imposed on small and big companies across all industries. Since the majority of these Privacy and Data Protection laws are quite new, case law is still rare, which leads to the fact that also courts have recently become more active in clarifying open questions and interpretations in the Privacy and Data Protection space. Besides that, the realm of Privacy and Data Protection is constantly broadening. Not only in the Privacy space but also in connected fields such as Data Responsibility, Artificial Intelligence and Digital Ethics more and more laws, regulations and guidelines are being enacted, and new forms of enforcement being introduced.

These extremely fast-paced global Privacy and Data Protection developments are challenging for all stakeholders. Global-acting companies, for example, are required to follow these deve-

lopments in all relevant jurisdictions continuously, in a timely manner and they need to implement the respective legal and compliance requirements promptly and comprehensively. However, in order to make sure that a company and its Privacy and Data Protection Compliance Program stays on top of all these new developments and fast-paced changes, a company needs mostly three things: great talent, a comprehensive program, and executive leadership commitment.

A great Privacy Team: First of all, it is important to have great Privacy talent on board. Especially companies with an international footprint and a multi-national user base, benefit from Privacy professionals with diverse jurisdictional, cultural and linguistical backgrounds. Besides that, it is also recommended to hire Privacy talent with different professional backgrounds, i.e. not only Privacy lawyers but also talent with specific Information Security, Engineering, Artificial Intelligence, Marketing, Advertising, Project Management, Customer Service and Compliance and Regulatory experience.

A comprehensive Privacy Program: Second, with a great team, a company can build a robust, comprehensive and sustainable Privacy and Data Protection Program. Such a Program comprises, for example, the areas of Privacy request management, fulfilment of user rights, Privacy documentation and risk assessments, data sharing and safeguarding of international data flows, Privacy by design and default, Privacy trainings and awareness, data deletion and data retention, as well as the correspondence and cooperation with Supervisory Authorities.

Executive leadership commitment: This is the most important piece. In order to implement Privacy compliance successfully across the board, for example Privacy by design and by default, a company's executive leadership team needs to be fully aware and committed. It is important to keep in mind that Privacy and Data Protection compliance is not only the responsibility of the company's Privacy or Data Protection Team – it is actually everyone's responsibility, from the CEO to the intern. Everyone in a company needs to be aware and trained how user and employee data can and must be protected on a daily basis.

La privacidad y la protección de datos son temas extremadamente candentes. Casi todas las semanas se aprueban nuevas normas de privacidad y protección de datos, las Autoridades supervisoras se han vuelto más activas, y casi todos los días podemos leer en los medios noticias sobre multas elevadas que se imponen a pequeñas y grandes empresas en todas las industrias.

Para asegurarse de que una empresa y su Programa de Cumplimiento de Privacidad y Protección de Datos Personales estén al tanto de todos estos nuevos desarrollos y cambios vertiginosos, una empresa necesita principalmente tres cosas: gran talento de profesionales de privacidad con diversos antecedentes jurisdiccionales, culturales y lingüísticos, un programa de privacidad integral, y el compromiso de liderazgo ejecutivo para que todo el personal de la empresa este consciente y comprometido con el cumplimiento de la privacidad y la protección de datos personales.

Barbara Cosgrove

VP, Chief Privacy Officer, Workday.
@barb_cosgrove
LinkedIn Barbara Cosgrove

As a leader in cloud applications for finance and human resources, Workday's top priority is to protect the privacy and security of our customers' data. It is imperative that we comply with global data protection laws and establish trust with our customers. The roles of the Chief Privacy Officer and Data Protection Officer (DPO) are key to that function. At Workday, the DPO provides trusted oversight over the processing of personal data and helps keep the company steered in the right direction when making data processing decisions.

Internal or External DPO

True to our core values of integrity and innovation, Workday determined that the best approach for our company would be to build out its own internal data protection office, as opposed to using an external DPO. For the DPO to successfully oversee and make recommendations to internal stakeholders about the interpretation of data protection laws, we established an internal function. By embedding this independent function within the business, the DPO can deeply understand Workday's technology, organization, and processes. This enables the DPO to respond more quickly to questions posed by individuals or data protection authorities and help ensure that we act as a trusted partner to our customers.

Independent Structure

The DPO must have autonomy and access to every level and role in the organization to fulfill its supervisory and enforcement obligations. With that in mind, we built out an Office of the Chief Privacy Officer, which is an independent organization reporting into our Chief Legal Officer (CLO). Our CPO is in the United States, and our DPO and Deputy DPO are located in Ireland, at our European headquarters. They are prepared to engage with any data protection regulator, where required and not just the lead regulator. The DPO independently meets with the CLO to provide regular updates on matters and can connect directly with the co-CEOs and Board of Directors when necessary. The CPO, DPO and the head of the Privacy team provide a formal privacy update to the Board of Directors at least once a year.

Making Relationships a Priority

To be effective, the DPO must build trusted relationships internally and externally. Internally, the DPO must be engaged with the teams that advise on internal processing and must oversee training content and delivery. In addition, the DPO must build strong relationships with data protection authorities around the globe, as well as peers to share best practices.

Scaling to Address Global Regulations

As global privacy regulations rapidly evolve and innovation requiring the use of data similarly continues to gain momentum, it's more important than ever for global technology companies to evaluate how they are building out their DPO function. Our office of the CPO

is global in nature and is composed of experts with in-depth knowledge of data protection regulations. To help this global function operate efficiently, it's also critical to invest in compliance frameworks and certifications to assist this role in providing regular oversight of the business. At Workday, we employ various mechanisms to demonstrate data protection compliance. As examples, we helped develop and were the first company to certify adherence to the European Cloud Code of Conduct, which demonstrates compliance with the GDPR, for declared services. We have binding corporate rules for processors, APEC Privacy Recognition for Processors, and ISO 27018 Certification. By coupling these third-party compliance mechanisms with our DPO's regular internal and external engagement activities, Workday is well equipped to be a trusted partner to our customers and their users, and cooperate with data protection authorities.

Como líder en aplicaciones en la nube para el sector de las finanzas y recursos humanos, la principal prioridad de Workday es proteger la privacidad y seguridad de los datos de nuestros clientes. Es imperativo cumplir con las leyes globales de protección de datos y establecer confianza con nuestros clientes. El rol del DPO es clave para esta función brindando una supervisión confiable sobre el procesamiento de datos personales y orientando las decisiones sobre el procesamiento de datos.

Fieles a los valores de integridad e innovación, Workday determinó que el mejor enfoque para la empresa sería construir su propia oficina interna de protección de datos, que cuenta con autonomía y tiene acceso a todos los niveles organizacionales, para así cumplir sus obligaciones de supervisión y ejecución en materia de datos e interactuar en conjunto con cualquier regulador global de protección de datos.

Lara Kehoe Hoffman

Vice President of Privacy and Security (legal) and Chief Privacy Officer at Netflix.

Netflix is streaming in more than 30 languages in 190 countries. We believe great stories can come from anywhere and be loved everywhere. Examples include: *Stranger Things*, *La Casa de Papel*, *The Crown*, *Lupin*, and *Squid Game*.

We are an entertainment company where deep human expertise and machine learning techniques work hand in hand to create a personalised experience that is focused on helping you find content of interest to you.

When you log into your Netflix account and land on your homepage, you are only seeing the tip of the iceberg of a vast and diverse catalogue. There are thousands of movies and TV shows available to watch, and many of them are new stories. This means we need a way to help you discover content that will delight you and your nuanced and diverse content tastes.

So we offer the ability to browse by genre, search for a title, and see what's popular. We also make recommendations based on what we think you may like. In the end, you get to choose and control what you want to watch.

How do we think about our recommendations:

• We want them to be accurate in that they are relevant, and they also need to be diverse so that we can address the spectrum of your interests versus only focusing on one.

• We want to be able to highlight the depth in the catalogue we have in your interests and also the breadth we have to help you explore and find new interests.

• We want our recommendations to be fresh and responsive to the actions you take, such as watching a show, adding something to your list, or giving something a thumbs up or thumbs down.

So what does storytelling have to do with being a data protection officer?

Data is useful and important in making recommendations that help entertain the world. The job of a DPO is to ensure that data is used responsibly.

It's important for the rules around responsible use to be clear for audiences throughout a company. But those rules must also allow for flexibility to support different business models. And ideally as a DPO you want to be able to harmonise those rules across different regimes. Ambiguous mandates and unique, wildly different approaches introduce a lot of complexity as you think through a compliance strategy. The more complexity there is, the more likely compliance systems are to fail.

As data protection officers we each need to be an independent voice, a data subject focused advocate, who tells the story of data protection and helps our organisation choose it again and again.

• We and our teams are responsible for understanding the current regulatory landscape and member expectations, how these are likely to change, and what are and will be the expectations of our organisation as it operates within those environments.

• We also need to understand the business - what is the company culture, what are the core goals, who are the decision makers, who are the influencers, who does the implementation.

• And we need to join these understandings into digestible guidance for different parts of the organisation and clearly communicated notices and choices for individuals whose personal data we collect and use.

Thank you to the Global Privacy Assembly for the opportunity to share these thoughts.

Netflix es una empresa de entretenimiento donde la profunda experiencia humana y las técnicas de aprendizaje automático trabajan de la mano para crear una experiencia personalizada que se enfoca en ayudar a las personas a encontrar contenido de su interés.

Los datos son útiles e importantes para hacer recomendaciones que ayuden a entretener al mundo. El trabajo del DPO es garantizar que los datos se utilicen de manera responsable, así como:

• Somos responsables de comprender el panorama regulatorio actual y las expectativas de los miembros.

• Entender el negocio.

• Y debemos unir estos entendimientos en una guía digerible para las diferentes partes de la organización, y avisos y opciones claramente comunicados para las personas cuyos datos personales recopilamos y usamos.

Gracias a la Asamblea de Privacidad Global por la oportunidad de compartir estos ideas.

Takeshige Sugimoto

Managing Director at S&K Brussels LPC,
Co-Founder and Member of Board of Directors at Japan DPO Association
Linkedin Takeshige Sugimoto

Do we understand how people feel? How does the privacy stay relevant?

I believe I'm the only external DPO on this panel, and so, I'd like to take this opportunity to contribute to this panel by sharing my observations and experiences as an external DPO.

To start off, I'd like to make a few remarks on the roles of DPOs.

1. First, DPOs are at the heart of the global data protection regime for many organizations, facilitating compliance with the provisions of each data protection law in the world. As the Article 29 Working Party rightly argued before the adoption of the GDPR, it is undeniable that the DPO is a cornerstone of accountability and that appointing a DPO can facilitate compliance and, furthermore, become a competitive advantage for businesses.

2. Second, such roles of DPOs have been achieved so far in many organizations because it is ensured that DPOs are able to perform their tasks with a sufficient degree of autonomy within their organization and that DPOs, whether or not they are an employee of the controller/processor, are in a position to perform their duties and tasks in an independent manner.

3. Third, as a future proof, I believe that the roles of DPOs will only be expanded even more dynamically across wider jurisdictions and not the other way round. For instance, China has just introduced the obligation to appoint a personal information protection officer into their new China PIPL. Also, in the US, both Democrat and Republican Senates have been working together to adopt a comprehensive federal data privacy law in congress. In both the U.S. federal data privacy bills of Democrat's COPRA and Republican's SAFE DATA Act, there appears to be an agreement between both parties to introduce obligations to appoint a data privacy officer into future U.S. federal privacy law.

4. Fourth, I'd like to emphasize the significant skills, experience and professionalism that DPOs can bring. The DPO role under GDPR has also enabled more effective provision of independent advice within organizations and visibility in corporate governance at board level.

5. Last but not least, DPOs across the globe can work together as colleagues of relevant stakeholders such as supervisory authorities, data subjects, and business units within an organization. DPOs can act as intermediaries among those stakeholders to help each stakeholder understand how the other stakeholders feel about certain processing of personal data in order to fill in the gaps among them to further promote data protection.

What are the challenges of adapting a data protection model to multiple jurisdictions and regulations?

1. While there are various challenges of adapting a data protection model to multiple jurisdictions and regulations, many organizations have a single set of internal data protection rules that apply globally across the entire organizational group, given that national data protection laws have extraterritorial provisions and regulate the cross-border transfer of personal data.

2. I think that one of the most common approaches among such organizational groups is to have two tiers of rules: first, a single set of internal data protection rules that apply globally across the entire organizational group, and secondly, a set of country-specific rules that only apply to sites in the relevant country to deal with matters specific to each country's legislation.

3. Of the two, I believe there are considerable challenges in establishing and implementing a single set of internal data protection rules that apply to an entire organizational group. Many organizations find that the rules become irrelevant if they do not have the necessary resources to comply with a single set of internal data protection rules that apply to the entire organizational group. In this regard, I believe that DPOs can work effectively within organizations to establish and enforce such rules.

4. From an external DPO standpoint, obtaining approvals from regulators for the Binding Corporate Rules, or BCRs, under the EU/UK GDPR, and implementing those BCRs is indeed very powerful in promoting data protection in large organization groups because EU/UK BCRs would truly increase data protection within organization groups by requiring the development and implementation of a rigorous employee training plan, internal audit structure and audit schedule and much more.

Al ser el único DPO externo en este panel, me gustaría aprovechar esta oportunidad para contribuir compartiendo algunos comentarios en específico.

1. Los DPO están en el centro del régimen global de protección de datos para muchas organizaciones, lo que facilita el cumplimiento de las disposiciones de cada ley de protección de datos en el mundo.

2. Se debe garantizar que los DPO pueden realizar sus tareas con un grado suficiente de autonomía dentro de su organización y estén en condiciones de desempeñar sus funciones y tareas de manera independiente.

3. La importancia del DPO es tal, que existen acuerdos para nombrar a un oficial de privacidad de datos en las futuras leyes.

4. El rol de DPO bajo el GDPR también ha permitido una provisión más efectiva de asesoramiento independiente dentro de las organizaciones y visibilidad en el gobierno corporativo.

5. Los DPO pueden actuar como intermediarios entre las partes interesadas para ayudar a cada parte a comprender cómo se sienten acerca de cierto procesamiento de datos personales para llenar los vacíos entre ellos y promover aún más la protección de datos.

The status of COE 108+ and the prospects of a COE Treaty on AI

Veronique Cimina

Legal officer at European Data Protection Supervisor (EDPS).
@VeroCimina and LinkedIn Veronique Cimina

The panel on '***The status of COE 108+ and the prospects of a COE Treaty on AI***' aimed at exploring the status of Convention 108+, while also identifying the possible prospects of a Council of Europe Treaty on Artificial Intelligence.

The panel was moderated by Veronique Cimina (European Data Protection Supervisor), and featured four esteemed speakers:

• Gonzalo Sosa Barreto**,** Data Protection Coordinator at the Regulatory and Control of Personal Data Unit (Uruguay);

• Paul Breibarth, Former Director of the Global Policy & EU Strategy at TrustArc;

• Alessandro Mantelero**,** Associate Professor of Private Law and Law & Technology at the Polytechnic University of Turin;

• Jean-Philippe Walter, Data Protection Commissioner at Council of Europe and a Member of the ICRC Data Protection Commission.

Firstly, the panel explored whether Convention 108+ has the capacity of becoming a global standard. While it appears that Convention 108+ is not always fully known within the private sector, the panel agreed that it is one of the main data protection instruments available, therefore resulting in an increased capacity of becoming a global standard.

Secondly, the discussion focused on providing a brief history on the development of Convention 108+, together with its main strengths in comparison with Convention 108. Moreover, it also noted the Council of Europe's contribution to the data protection and privacy legal framework when using AI systems. In this context, discussions mainly highlighted the issue of data quality and bias.

Thirdly, the panel guided the audience through the similarities and complementarity of data protection and future AI regulations in the Council of Europe context, particularly by reflecting on its interaction with the (then) recently proposed AI Regulation by the European

Commission. The discussion on this matter not only underlined the importance of Convention 108+ and the elements it already provides for, but also the essentiality of risk management and risk assessment in addition to data protection.

Lastly, the discussion focused on the interaction and convergence of Convention 108+ with other international standards (and particularly Latin America), while also providing for an assessment on the effects of the Council of Europe's legal framework and its development within private practice.

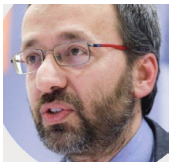
Overall, the panel, not only provided for an assessment of the status of Convention 108+ and on the possible prospects for a Council of Europe's Treaty on AI, but also highlighted the priorities and biggest challenges for the Council of Europe in the years to come, including the fundamental importance of reaching a substantial number of ratifications to Convention 108+.

El panel proporcionó una evaluación del estado del Convenio 108+ precisando sobre la capacidad de convertise en un estándar global, y proporcionó una breve historia sobre el desarrollo del Convenio 108+, junto con sus principales fortalezas en comparación con el Convenio 108.

Así mismo se debatió sobre las posibles perspectivas para un Tratado del Consejo de Europa sobre Inteligencia Artificial, particularmente reflexionando sobre su interacción con la (entonces) recientemente propuesta de Regulación de IA de la Comisión Europea, al tiempo que también destacó las prioridades y los mayores desafíos para el Consejo de Europa en los años venideros, incluyendo la importancia fundamental de alcanzar un número sustancial de ratificaciones al Convenio 108+.

Alessandro Mantelero

Chair in Mediterranean Digital Societies and Law, Polytechnic University of Turin



From data protection to AI in the prism of the Council of Europe

The new leaps in AI and the unrelenting datafication of society and physical world have been key drivers of a renewed interest in data protection on the part of legislators. Lack of regulation, outdated models, overestimation of individual dimension and consent, and the increased complexity of global data flows are some of the main factors that have led to a modernisation of legal frameworks.

The most prominent feature of this new generation of data protection regulations is the preference for a holistic approach, as in Convention 108, which is borne out by the ongoing debate in the US, where the traditional sectoral approach has given way to proposals focused on a general federal data protection regulation.

The evolving socio-technical scenario has challenged the existing data protection framework and required specific changes. This was the case with the modernised version of Convention

108, which aimed to overcome the limitations of a model rooted in the socio-technical context of the late 1970s.

Although the modernised Convention introduces important changes, particularly in the areas of risk management, new AI-based applications raise issues that go beyond the protection of personal data and call for complementary principles and provisions specifically designed for AI.

The Council of Europe (CoE) was the first forum where we saw the emerging of a new approach to address these urgent challenges posed by AI, not relying solely on ethical principles, but focusing on legal principles grounded in human rights, the rule of law and democracy.

Looking at the trajectory developed by the CoE since the establishment of the Ad hoc Committee on Artificial Intelligence (CAHAI), from the initial ambitions to set up a legal framework for AI based on CoE standards on human rights, democracy and the rule of law —which recalled experiences such as the Oviedo Convention and Convention 108— to its current outcome (Ministers' Deputies, Decisions, CM/Del/Dec(2022)1425/10.1, Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law), the result achieved does not seem to fully meet the initial ambitions.

While there is no doubt about the merits of the CoE in emphasising the importance of adopting a legally binding instrument for AI and focusing on human rights, the draft document does not provide a comprehensive set of principles and provisions suitable to guide the development of AI, nor does it offer a risk-based approach built on a sound assessment model. Several critical issues remain unaddressed with regard to the scope of the future convention on AI, the use of AI in the public sector, red lines, and the risk-based approach (Mantelero-Fanucci, 2022. In Philip Czech et al. (eds). European Yearbook on Human Rights 2022).

Echoing the DPIA models, the CoE departs positively from the EU's AIA approach —which is centred on a risk classification provided by law— and adopts a two-step model based on an initial review to determine if a full HUDERIA (Human Rights, Democracy and Rule of Law Impact Assessment) is required. However, crucial limitations affect the HUDERIA itself.

First, while there is significant experience with impact assessment in the field of human rights, the inclusion of democracy and the breadth of its various forms make impact assessment methodologically difficult, even more so as it is hard to assess the level of democracy itself.

Second, the HUDERIA model seems challenging in its transition from theoretical formulation to concrete implementation as the emphasis on risk management is not accompanied by effective models to assess the impact of AI on human rights (Mantelero, Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI. Springer, 2022).

Finally, although the CoE has supported the active involvement of stakeholders in the assessment process, it did not provide specific indications on the transparency of the assessment process and its results.

Looking at the experience of data protection regulation —and, more specifically, Convention 108—, it is therefore crucial both to provide and effective and principles-based framework for AI (not limited to risk management) and to benefit from the principles, safeguards, and practices that already exist in the field of data protection, avoiding any improper overlap in regulating data-intensive AI applications.

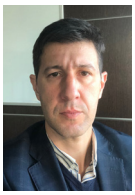
Los nuevos adelantos en Inteligencia Artificial y la increíble datificación de la sociedad y del mundo físico, han sido impulsores de un renovado interés en la protección de datos personales por parte de los legisladores. La falta de regulación, los modelos obsoletos, la mayor complejidad en el flujo de datos globales, son algunos de los factores que han llevado a una modernización de los marcos legales.

La característica más destacada de esta nueva generación es la preferencia por un enfoque holístico, como en el Convenio 108. Las nuevas aplicaciones basadas en IA plantean problemas que van más allá de la protección de los datos personales y exigen principios y disposiciones complementarios diseñados específicamente para esta tecnología.

Es crucial proporcionar un marco efectivo basado en los principios de la IA y beneficiarse de los salvaguardas, y prácticas que ya existen en el campo de la protección de datos personales.

Gonzalo Sosa Barreto

Data Protection Manager - URCDP



Uruguay's Data Protection Authority

The impact of Convention 108 and 108+ on the Uruguayan Regulation.

As everyone in the world of data protection knows, Convention 108 was adopted and opened for signature in Strasbourg on January 28, 1981 —the date on which It is currently commemorated at the international level, the "Data Protection Day"—.

Uruguay was the first non-European country to be part of the Convention and its Additional Protocol of 2001, and the first Latin American country to sign, and later formally adhere to, its modernization protocol (Convention 108+).

The motivations for the original adhesion of Uruguay are based on a neuralgic point, which is the consideration of the right to the protection of personal data as a fundamental right. Likewise, the regulation in the Convention of basic principles of data protection is central, in order to facilitate the secure exchange of personal information between the Parties, establish cooperation mechanisms between independent authorities, and ultimately promote the implementation of an adequate level of data protection at a global level.

Uruguay's adherence to the modernization protocol is also explained in the synergies of the different international and regional instruments, which are identified with a set of improvements associated with the obligations of the parties, the standards of data protection, enforcement mechanisms, the role of the Consultative Committee, among others.

Moreover, being part of the Convention ensures its members the participation in an international discussion forum on the most pressing issues in the matter, made up of authorities, experts and organizations, and the generation of networks of cooperation and collaboration, essential in the current world.

The work of the Consultative Committee, and the preparation of documents, opinions and other instruments is essential to understand the transversal role of data protection in all areas of human activity. And its effects, derived from the universal vocation of the Convention, transcend the European sphere, impacting in other regions. The growing participation of authorities from Latin America, Africa and Asia demonstrates this, as well as the carrying out of different activities by the Consultative Committee in countries of those regions to collaborate with national and regional initiatives on data protection.

In the coming years there are challenges that must be faced; the first is to promote the adherence of more States parties -and others- to the new modernization protocol, which requires compliance with certain requirements expressly provided for its entry into force. The proposed changes, which are of absolute relevance and necessity to continue working on a protective data protection ecosystem for people regardless of their place of residence, and which are associated with the new standards of the modernization protocol, need to be endorsed by the parties through their adherence to this necessary instrument.

It is also essential to incorporate the precepts included in the new provisions —aligned with regulations such as the General European Data Protection Regulation (GDPR) and with standards such as the Standards for Ibero-American States of the Ibero-American Data Protection Network (RIPD)— in the different national legislations of the member states, in order to obtain greater harmonization at a global level. And this because harmonization by itself is not enough to ensure the due protection of people, but rather it must be associated with higher standards, such as those proposed by Convention 108+.

For example, in Uruguay, inspired among others by Convention 108+, the RIPD standards and the GDPR, Law No. 19.670, of October 15, 2018, established important changes in the legislation, with a new communication regime of security breaches, the consecration of proactive responsibility as a principle and the figure of the data protection officer, and the creation of an extraterritorial application system of the law. Then Law No. 19.924, of December 18, 2020, included in the national regulation the concept and specific requirements for biometric data processing, and finally Law No. 19.948, of April 27, 2021, incorporated Convention 108+ into national legislation.

It will be a challenge within the framework of Convention 108+, to work on making the planned cooperation mechanisms effective, as this is essential for proper enforcement of the different regulations on the matter. Also, to collaborate in ensuring the defense of this right, incorporating provisions on data protection within the different Conventions of the Council of Europe, and outside of it; and continue working with national authorities and regional and global organizations to generate networks and synergies.

We will continue to monitor the development of the activities of the Consultative Committee of Convention 108, convinced of its relevance and its impact to ensure the rights of people, through the protection of their data.

Uruguay fue el primer país no europeo en formar parte del Convenio 108 y su Protocolo Adicional de 2001, y el primer país latinoamericano en suscribir, y posteriormente adherirse formalmente a su protocolo de modernización, el Convenio 108+. Las motivaciones para la adhesión de Uruguay se sustentan en un punto neurálgico, que es la consideración del derecho a la protección de datos personales como un derecho fundamental.

En los próximos años existen desafíos que deben ser encarados; el primero es promover la adhesión de más Estados parte —y de otros— al nuevo protocolo de modernización, que requiere del cumplimiento de determinados requisitos expresamente previstos para su entrada en vigencia.

Seguiremos atentos el desarrollo de las actividades del Comité Consultivo del Convenio 108, convencidos de su relevancia y de su impacto para asegurar los derechos de las personas a través de la protección de sus datos personales.

Jean-Philippe Walter

Data Protection Commissioner, The Council of Europe

Convention 108+, a first rate paper in the digital and artificial intelligence era.

Convention 108 is an open treaty from its origin, which is not exclusive for European countries. The text, ratified by 55 States, is still the only legally binding instrument on the subject of data protection and is open to adherence by non-European States. This openness intention was reinforced with the updating of Convention 108 which led to Convention 108+, which may be described as an international data protection instrument with a global scope. Aside from adhesion, the Convention has a strong influence, mainly in the preparation of domestic and regional laws.

Convention 108+, a first rate paper in the digital and artificial intelligence era. It allows to offer a data protection level corresponding international standards accepted and recognized by countries and regional organizations, particularly by the European Union, to any person under the jurisdiction of a party. Thus, it guarantees human rights and fundamental liberties, particularly, the right to privacy of each and every person, including respect for human dignity and personal autonomy. These fundamental values, as linked to data protection, are essential in the debate on AI.

With these moderate and flexible rules, Convention 108+ establishes the minimum, while high, commonly accepted protection level that any person shall enjoy in the digital era. It is a sustainable tool to simplify international data transfers while ensuring an adequate level of data protection for people at a global level.

People's trust in personal data processing is essential for public and private sector's data processors, governments, and economic actors. This confidence is based on an adequate level of protection. Facing diverse legal resolutions, particularly those of the CJEU that

invalidate data transfer agreements due to a lack of guarantees on the rights of those involved, Convention 108+ may effectively contribute to ensure a high level of protection worldwide.

Convention 108+ can also support corporations to function and interact more freely, without limitations on data export and import. In a highly independent global economy, growingly centered in data, the Participant States may guarantee an ideal legal framework and global environment for economic and commercial activities that enforce universally recognized human rights. Being part of the Convention is an important element to be considered by the European Union to issue a compliance resolution.

Also, the States and International Organizations participating in the Convention are bound to mutual cooperation to guarantee the highest level of data protection as well as a perfect fulfillment of international standards. All countries and organizations that adhere to Convention 108+ participate in the development of the right to data protection at a multilateral level while contributing to maintain the free circulation of data worldwide.

Convention 108+ is the benchmarking instrument on the subject of personal data protection. This, at a global scope and for data processing within the context of artificial intelligence systems. Thus, the new discussion or preparation instruments should not risk current achievements or weaken the provisions and principles of Convention 108+, which offers a strong and balanced legal framework to guarantee fulfillment of the right to data protection in AI systems. The greatest challenge for Convention 108+ and data protection regulations within the scope of AI is to obtain its ratification from at least 38 Participant States by 2023 and begin its aligned application.

It is therefore urgent that all the Parties of Convention 108 take part in Convention 108+ It is strictly necessary that it becomes effective rapidly to enable the application of its evaluation mechanism and cooperation between data protection authorities. Data protection authorities and the GPA shall actively support a rapid ratification.

El Convenio 108 ratificado por 55 Estados, sigue siendo el único instrumento jurídicamente vinculante en materia de protección de datos a nivel mundial y está abierto a la adhesión de Estados no europeos. Esta intención de apertura derivó en el Convenio 108+, que puede describirse como un instrumento internacional de protección de datos de alcance global.

La Convención 108+ garantiza los derechos humanos y las libertades fundamentales, en particular, el derecho a la intimidad de todas y cada una de las personas, incluido el respeto a la dignidad humana y la autonomía personal. Estos valores fundamentales, vinculados a la protección de datos, son esenciales en el debate sobre la inteligencia artificial.

Así, los nuevos instrumentos de discusión no deben poner en riesgo los logros actuales ni debilitar las disposiciones y principios del Convenio 108+, que ofrece un marco legal sólido y equilibrado para garantizar el cumplimiento del derecho a la protección de datos en los sistemas de IA. Su mayor desafío es lograr su ratificación en al menos 38 Estados Participantes para el 2023 y empezar su aplicación.

Paul Breittbarth

Data Protection Lead, Catawiki & Senior Visiting Fellow, Maastricht University's European Centre on Privacy and Cybersecurity

Convention 108+: Also important from a business perspective

Since the Schrems-II decision of the Court of Justice of the European Union (EU), the business community is in uproar. Data transfers, especially those from the EU to the United States, have become a lot more complicated. But also, other jurisdictions are taking a renewed interest in which requirements to put in place when transferring personal data across borders. Can indeed be guaranteed that the data will be protected like at home? This is of course a key interest for every individual.

While bilateral agreements, especially those declaring the data protection regime in other jurisdictions as *adequate* may be part of the solution, the real solution can only come from a binding international arrangement. A treaty or convention that binds countries to a high level of data protection, and that ideally also encompasses any data processing by the intelligence and security community, would give individuals the protection of their fundamental rights like they deserve.

Does that mean we need to spend years negotiating a new agreement, taking attention away from all the other data protection related work that may be required, with the chance nothing ever materialises? No, luckily not, because that agreement was already negotiated: it is the Council of Europe Convention 108+. Convention 108+ has the unique opportunity to become the global standard on personal data protection: it allows for accession by any country that wishes to do so. And coming from a body that has fundamental rights at its core, it also ensures a very high level of protection. From my European perspective, the Convention would even more be a great solution, since it aligns so well with the GDPR.

It is therefore an evident business interest that Convention 108+ is quickly ratified and that the group of countries acceding to the Convention increases, also beyond the member countries of the Council of Europe. Only this way we can create the legal certainty that companies so much need to continue to do business on a global scale, while having the legal options to ensure a high level of data protection for the data they process.

Desde la decisión Schrems-II del Tribunal de Justicia de la Unión Europea (UE), la comunidad empresarial está alborotada. Las transferencias de datos, especialmente las de la UE a los Estados Unidos, se han vuelto mucho más complicadas. Pero también otras jurisdicciones están volviendo a interesarse por los requisitos que se deben implementar al transferir datos personales a través de las fronteras. ¿Se puede garantizar que los datos estarán protegidos como en casa? Esto es, por supuesto, un interés clave para cada individuo.

Si bien los acuerdos bilaterales, especialmente aquellos que declaran adecuado el régimen de protección de datos en otras jurisdicciones pueden ser parte de la solución, la solución real solo puede provenir de un acuerdo internacional vinculante.

¿Eso significa que debemos pasar años negociando un nuevo acuerdo, desviando la atención de todo el trabajo relacionado con la protección de datos que pueda ser necesario, con la posibilidad de que nada se materialice? No, por suerte no, porque ese acuerdo ya estaba negociado: es el Convenio 108+ del Consejo de Europa. El Convenio 108+ tiene la oportunidad única de convertirse en el estándar mundial sobre protección de datos personales.

Parallel Sessions

Data Analytic users: considerations in privacy

Steve Wood

Allen and Overy special adviser on data protection. Deputy Information Commissioner. Policy development and regulatory strategy. ICO, UK.

Steve Wood raised the following points during his speech:

• **Scale and scope of data analytics** – data analytics increasingly drive public and private sector data processing and the pandemic has accelerated the digitalisation process.

• **The risks and challenges** – data analytics are shaping decisions that have significant implications on individuals and society, from medical treatment to recruitment, law enforcement to prosecutions.

• **The benefits of data analytics-driven processes** – the potential of personalisation offered by data analytics can provide more effective public and private services.

• **Data analytics and rights** – data analytics cut across and engage a number of different fundamental rights.

• **Realising the potential of data analytics through building public trust and confidence** – data protection and privacy laws can and should build public trust by enabling appropriate data processing and protecting the public.

• **Delivering transparency in practice** – data analytics providers need to better assess what users need and the importance of privacy by design and accountability.

Entre los temas abordados durante esta sesión paralela se encuentran:

• Escala y alcance del análisis de datos: el análisis de datos impulsa cada vez más el procesamiento de datos del sector público y privado y la pandemia ha acelerado el proceso de digitalización.

• Los riesgos y desafíos: el análisis de datos está dando forma a decisiones que tienen implicaciones significativas para las personas y la sociedad.

• Los beneficios de los procesos impulsados por el análisis de datos: el potencial de personalización que ofrece el análisis de datos puede brindar servicios públicos y privados más efectivos.

• Análisis de datos y derechos: el análisis de datos abarca y compromete una serie de derechos fundamentales diferentes.

• Aprovechar el potencial del análisis de datos a través de la creación de confianza y seguridad pública: las leyes de privacidad y protección de datos pueden y deben generar confianza pública al permitir el procesamiento de datos adecuado y proteger al público.

• Ofrecer transparencia en la práctica: los proveedores de análisis de datos deben evaluar mejor lo que necesitan los usuarios y la importancia de la privacidad por diseño y responsabilidad.

Caitlin Fennessy,

VP & Chief Knowledge Officer, International Association of Privacy Professionals

Historically, we have discussed data analytics and privacy in black and white terms. We have balanced the benefits of massive data collection and powerful analysis against the risks. We sat in camps celebrating data-driven innovation, defending over-collection in the name of safety, or lamenting a growing surveillance state. Many appreciated the continuum and nuances, but the debate has been polarized.

Today, I hope, we are moving toward a dynamic where we recognize and inject dials into every component of data processing, dials corresponding to longstanding resilient fair information practice principles. While the FIPPs terminology is used less frequently today than privacy or data protection, it may be better suited to the modern data-driven age.

Let me explain.

The United Kingdom recently launched a national data strategy to consider how data is used or could be used productively across the economy and society. They did not launch a privacy strategy or a data protection strategy, though their consultation is infused with the principles and questions with which we all are grappling. It considers data use and responsibility holistically. That is where I think our field is headed.

The privacy profession grew up in the legal domain. But today, only about one third of the IAPP's 75,000 members are lawyers. The rest are not thinking about data analysis in terms of legal compliance. They are thinking about data through an engineering lens, a business product lens, a user-interface design lens, a marketing lens, a data scientist lens. To them, the "collection limitation" principle is not about minimizing data collection to align with GDPR Article 5(1)(c). It is about where data is needed, where it is an asset, where it is a liability, where it is informing and where it is useless or worse yet damaging to the business and individuals. It is about aligning data collection, use and analysis with user expectations, with product strategy and with an understanding of the scope and limitations of the data itself.

In recent months, we have seen the incredible benefits of data analysis to drive innovation. COVID has provided us many examples – from vaccine development to health apps that help us identify the onset of the virus before symptoms appear. We have also seen the massive divisions and damage that can occur when data analytics change the information and opportunities we are exposed to. Sometimes, it feels like the power of data-driven decisions extends beyond organizations' abilities to control it.

Ultimately, it comes back to the people engaged in every stage of data analysis. Privacy by design can no longer be a process, spearheaded by legal and compliance alone. Increasingly, it should be a parlance and a question-set familiar to far more individuals across disciplines so that our products and services are conceptualized, engineered, displayed, marketed and fed back into strategy in a way that serves the business, individuals and communities in order to meet a layman's understanding of the term fair information practice principles. Only then will we see more creative and privacy-enhancing options around the collection, analysis and use of data.

Históricamente, hemos discutido el análisis de datos y la privacidad en términos de polarización, beneficios versus riegos, pero la realidad es que nos estamos moviendo hacia una dinámica en la que reconocemos que existen nuevos indicadores en todos los componentes del procesamiento de datos. Se trata de alinear la recopilación, el uso y el análisis de datos con las expectativas del usuario, con la estrategia del producto y con la comprensión del alcance y las limitaciones de los datos en sí.

Hemos visto increíbles beneficios del análisis de datos para impulsar la innovación. El COVID-19 nos ha brindado muchos ejemplos, desde el desarrollo de vacunas hasta las aplicaciones de salud que nos ayudan a identificar la aparición del virus antes de que aparezcan los síntomas.

La privacidad por diseño ya no puede ser un proceso encabezado sólo por aspectos legales y de cumplimiento. Debe ser un lenguaje y un conjunto de preguntas familiares para muchas más personas en todas las disciplinas. Solo entonces veremos opciones más creativas y que mejoren la privacidad en torno a la recopilación, el análisis y el uso de datos.

Daniel Leufer

Senior Policy Analyst at Access Now

The incredible growth in the amount of data produced, as well as the impressive development of techniques for analysing large amounts of data, has led to a boom in the field of data analytics. Machine learning, for example, has allowed us to process and derive insights from previously unmanageable amounts of data.

In responding to the growing prevalence of data analytics, digital rights advocates have often focused on data protection and privacy. While this is entirely legitimate, it can lead

to overlooking a more fundamental question of whether certain phenomena are even amenable to datafication and data analytics, and whether there are certain things that we simply cannot, and should not, be trying to predict.

To make this concrete, let's take the example of facial recognition technology (FRT). Considered broadly, the term FRT refers to a range of technologies which make predictions about images of people's faces. FRT can ask the question "is there a face in this image?" (facial detection) or "does this face match any of the faces in our watchlist?" (facial identification). In both cases, there is something like a 'ground truth' against which we can measure the performance of our system. In the case of facial detection, the image either contains a face or it doesn't, and with facial identification, the face in the image either belongs to a person on the watchlist, or it doesn't.

The existence of such a ground truth against which to measure the system's performance is key to highlight, because there are many other types of facial recognition which lack any such ground truth, and arguably lack scientific legitimacy for that reason.

An example of such a system is so-called emotion recognition. Many emotion recognition systems claim to be able to detect what emotion a person is feeling based on their facial expressions. However, these systems are typically based on simplistic theories that assume direct correlations between facial expressions (smile, frown etc.) and emotion states (happiness, anger), as well as assuming a global uniformity of discrete emotional states. The theoretical basis of such systems has been contested by many scholars across relevant fields, and there is no clear ground truth against which to evaluate a system's performance.

This problem becomes all the worse with systems that claim to predict things such as a person's suitability for a job, where facial recognition is used to predict things about a person's personality and likely job performance. There is no solid basis for making such inferences, and it can indeed be argued that making inferences about people's future behaviour, performance, or potential based on analysis of their facial expressions is a form of dangerous biological reductivism.

When thinking about data analytics, we should therefore not forget to question the basic legitimacy of the types of questions we are asking, and ensure that the data we produce, and the analysis we use it for, have a solid scientific basis.

En respuesta a la creciente prevalencia del análisis de datos, los defensores de los derechos digitales a menudo se han enfocado en la protección de datos y la privacidad. Si bien esto es completamente legítimo, pueden llegar a pasar por alto una cuestión más fundamental de si ciertos fenómenos son incluso susceptibles de datificación y análisis de datos, y si hay ciertas cosas que simplemente no podemos, y no deberíamos intentar predecir.

Es clave destacar la existencia de una "verdad básica" contra la cual medir el rendimiento del sistema, porque hay muchos otros sistemas que carecen de tal verdad y posiblemente carecen de legitimidad científica.

Al pensar en el análisis de datos, no debemos olvidar cuestionar la legitimidad básica de los tipos de preguntas que hacemos y asegurarnos de que los datos que producimos y el análisis para el que los usamos tengan una base científica sólida.

David Banisar

A human rights and information lawyer based in London, UK. Previously Senior Legal Counsel for ARTICLE 19, Deputy Director of Privacy International, and co-founder of the Electronic Privacy Information Center. LinkedIn David Banisar

Accountable data analytics and algorithms: The importance of transparency

The issue of analytics not a new problem for personal data. The collection, analysis, and use and misuse of personal information has been a concern since the beginning of mass computerisation of records, whether it was stored in databanks, registers, or big data, and the issue was data matching, data sharing, data mining, or machine learning going back to the 1960s in the US with the National Data Centre and the controversies in a number of European countries over centralized computer records. These debates led to the creation of the adoption of the US Fair Credit Reporting Act and the early data protection laws nearly 50 years ago and continue driving the increasing adoption and evolution of data protection laws now.

One measure that has long been promoted to ensure accountability of the processing of personal data is transparency. In data protection law, transparency has been incorporated as measures placing obligations on data processors to reveal the sources of their information, the uses they make of the information, and where it transferred to, and the right of subject access further offering access to information, protections and enforcement of the transparency rights. In modern laws, such as the GDPR, this has been further enhanced by obligations for algorithmic transparency and Privacy Impact Assessments.

Meanwhile, parallel to adoption of data protection laws, there has been a transparency revolution by countries to bring accountability to their own systems, both physical, and digital, by adopting national freedom of information laws which give individuals the right to obtain information from government bodies, and in some countries, such as South Africa, also private bodies where fundamental rights are affected. Today, over 130 countries have adopted these laws. These laws apply generally to all information and are increasingly used to demand information from government bodies on how algorithms are used to affect fundamental rights. But with that needs to be adequate enforcement. In a recent case in Poland on obtaining the algorithm used by the Ministry of Justice on how they choose judges for individual cases, the Ministry tried to claim that it was just administrative document, not something subject to FOI but were overridden by the Supreme Administrative Court in 2021.

The question is now how to ensure that transparency in machine learning and artificial intelligence is effective, to understand their biases and limitations and how those affect the decisions they make. Access to algorithms though DP and FOI laws is not enough. To be effective, there needs to be explanation so that how the systems work in practice is describable, including a description of their logic or access to the structure of the algorithms and —where applicable— to the datasets used to train the algorithms. Another important tool is public registers of algorithms so that the public, and officials, NGOs, and academic researchers, can track and monitor their use and implementation. And further, truly public procurement on the purchasing of these systems which reveal the purposes and operations of the systems.

Finally, transparency needs to be done hand in hand with effective accountability mechanisms. Beyond the current privacy impact assessment processes, which are often done in secret and not even made public, there should be a required mechanisms of public consultation before systems that impact widely on rights across communities can be implemented. Nearly every country in the world has adopted Environmental Impact Assessment (EIA) mechanism, so that when a dam or power plant or major road is built, the communities are consulted, and in the best mechanism, their views are taken into account and projects adjusted to ensure that the communities are not harmed. Other external mechanisms are also essential: oversight bodies, parliaments, law enforcement, strong consumer and citizens groups that can legally challenge, obtain the information and use.

Una medida que se ha promovido durante mucho tiempo para garantizar la responsabilidad del procesamiento de datos personales es la transparencia. Paralelamente a la adopción de leyes de protección de datos, ha habido una revolución de transparencia por parte de los países para llevar la rendición de cuentas a sus propios sistemas, tanto físicos como digitales, mediante la adopción de leyes nacionales de libertad de información que otorgan a las personas el derecho a obtener información de los organismos gubernamentales, y en algunos países, también entidades privadas donde se ven afectados los derechos fundamentales. Hoy, más de 130 países han adoptado estas leyes.

La pregunta ahora es cómo garantizar que la transparencia en el aprendizaje automático y la inteligencia artificial sea efectiva, para comprender sus sesgos y limitaciones, y cómo afectan las decisiones que toman.

Finalmente, la transparencia debe de ir de la mano de mecanismos efectivos de rendición de cuentas, como: organismos de supervisión, parlamentos, fuerzas del orden, grupos de consumidores y ciudadanos que puedan impugnar legalmente, obtener la información requerida y utilizarla.

Ed Britan

VP, Associate General Counsel, Global Head of Privacy, Salesforce. LinkedIn Ed Britan

It was a privilege to speak on this panel in October 2021, and I would like to thank both the co-panelists I spoke with, and the INAI and GPA for the opportunity. As the global leader of the Salesforce privacy team —a team that is truly global across many countries and continents— I was glad and honored to be speaking at this global event about this ever important topic, data analytics.

Data analytics are central to the global digital economy, and the information they produce can be powerful, and requires a thoughtful approach. Ineffective privacy protections, and improper use of data, can harm people and create liability for companies. As a large service provider, we know the importance of helping organizations manage and use their data responsibly, and effectively —protecting individual privacy is part of everything we do—. With this backdrop, I would like to highlight three points about how data analytics is changing, and can be more privacy protective and effective.

First, there are regulatory and market changes already shifting marketing analytics from third to first party data, which is more privacy protective. For example, companies like Apple and Google are following the regulatory trends set by the EU's GDPR, Brazil's LGPD, and California's CCPA and other recently-passed US state privacy laws, and restricting or planning to sunset third party cookies that track marketing analytics. That means companies are shifting towards using only data they personally collected about an individual for marketing purposes. And this is beneficial for strategic cookieless future planning reasons but also because it's more privacy protective, and allows individuals to better control their data.

Second, good data management protects privacy and helps fuel innovation and commerce. Individuals won't voluntarily share their data with companies that they don't trust. Thus, control and transparency are key for fostering the sharing of data that is necessary to produce effective data analytics. Providing more transparency, and individual choice and control over data, including through both granular and sweeping controls to enable individuals to prevent data collection and sharing, builds trust by allowing users to decide what data to provide for analytics. This in turn provides companies with the opportunity to effectively analyze important data.

Lastly, global datasets for use in data analytics are necessary both to drive business and positive societal change. We have heard that many organizations do not want their data to leave the EU, and recently announced the Hyperforce EU Operating Zone to enable organizations to address that concern. At the same time, there are ways to share data or insights from data across borders responsibly. For instance, Salesforce is part of the Trusted Cloud Principles, which was developed by the major public cloud providers and supported by Salesforce and Slack, and specifies important principles that companies are committed

to upholding to ensure responsible data flows and challenge improper government requests to access data.

As the Japan government has posited in our Data Beyond Borders 2.0 report, trusted data flows are possible. But it will require governments, companies, and civil society coming together to develop global frameworks for responsible data sharing and use. I look forward to those conversations, and conversations about privacy protective data analytics, as they will be critical for fostering responsible data practices globally.

El análisis de datos es fundamental para la economía digital global, y la información que producen puede ser poderosa y requiere un enfoque reflexivo. Las protecciones de privacidad ineficaces y el uso indebido de los datos pueden dañar a las personas y crear responsabilidades para las empresas. En Salesforce, siendo un gran proveedor de servicios, sabemos la importancia de ayudar a las organizaciones a administrar y usar sus datos de manera responsable y efectiva: proteger la privacidad individual es parte de todo lo que hacemos.

Me gustaría resaltar tres puntos sobre cómo está cambiando el análisis de datos y cómo puede ser más efectivo para la privacidad.

Primero, hay cambios regulatorios y de mercado que ya están cambiando el análisis del marketing de datos de terceros a datos de primera mano, lo que protege más la privacidad. Las empresas se están inclinando hacia el uso exclusivo de los datos que recopilaron personalmente. En segundo lugar, una buena gestión de datos protege la privacidad y ayuda a impulsar la innovación y el comercio. Y por último, los conjuntos de datos globales para su uso en el análisis de datos son necesarios tanto para impulsar el negocio como el cambio social positivo.

Espero con interés estas conversaciones sobre el análisis de datos de protección de la privacidad, ya que serán fundamentales para fomentar prácticas de datos responsables a nivel mundial.

Eduardo Ustaran

Partner at Hogan Lovells. eduardo.ustaran@hoganlovells.com.

Testing the legal boundaries of data analytics and privacy

Internet innovation is in a state of flux. New laws and proposals around the world are focusing on the protection of privacy and data in the digital economy. Against this background, the commercial urge to benefit from the use of data has never been greater. Therefore, one of the most important strategic questions for digital businesses right now is how to justify the use of data analytics in compliance with existing and emerging laws.

The GDPR in particular, with its intricacies around the lawful grounds for processing, has become a perfect testing ground for establishing the legitimacy of data analytics when accessing Internet-based content and services. In other words, under the GDPR, what is the soundest legal basis to undertake sophisticated analytics involving personal data? An

obvious answer may, of course, be consent. But the legitimacy of consent as a realistic ground for data processing in a world where we have lost much control over the uses of that data is constantly being questioned. Are we, humble Internet users, truly in a position to make an informed decision about data crunching practices that fly many, many miles over our heads? In short, do we have a genuine choice? Will we ever?

Given the pre-eminence and ever-growing importance of data analytics in the digital economy, it is crucial to find a more sophisticated approach to ensure that the legal basis for data analytics practices is as solid as its commercial justification. An increasingly popular fall-back position when consent is challenged as a lawful ground is 'legitimate interests'. Seen as a panacea for justifying data uses by many but misunderstood by most, the legitimate interests ground is certainly available for pretty much every commercial use of personal data. But it comes with strong conditions which, in the context of data analytics involve careful thinking about potential privacy intrusions, actively embracing data minimisation and integrity, and above all challenge-proof transparency and control. In a nutshell, 'legitimate interests' can go a long way to legitimise data analytics but it is crucial not to see it as a 'get out of jail free' card and to appreciate the considerable privacy-enhancing efforts that need to be made when relying on it.

On a practical level, our principal job is to embed privacy and cybersecurity practices in the development and implementation of data analytics. Key new legal principles such as data protection by design and by default should guide this process whilst allowing for pragmatism and common sense. Ultimately, getting this right is a matter of balance. It is about achieving the best of all possible worlds: control over our data and our digital lives on the one hand, and access to affordable and relevant products and services on the other. Those who get this right will be the most successful innovators of all.

La necesidad comercial de beneficiarse del uso de datos nunca ha sido mayor. Por lo tanto, una de las preguntas estratégicas más importantes para los negocios digitales en este momento es ¿cómo justificar el uso de análisis de datos de conformidad con las leyes existentes y emergentes?

Dada la importancia cada vez mayor del análisis de datos en la economía digital, es crucial encontrar un enfoque más sofisticado para garantizar que la base legal de las prácticas de análisis de datos sea tan sólida como su justificación comercial.

Nuestro trabajo principal es incorporar prácticas de privacidad y ciberseguridad en el desarrollo e implementación de análisis de datos. Los nuevos principios legales clave, como la protección de datos desde el diseño y por defecto, deberían guiar este proceso al tiempo que permiten el pragmatismo y el sentido común. Se trata de lograr lo mejor de todos los mundos posibles: por un lado, control sobre nuestros datos y nuestras vidas digitales, y por el otro, acceso a productos y servicios asequibles y relevantes. Aquellos que lo logren serán los innovadores más exitosos de todos.

United Nations Agenda 2030: The protection of personal data

Adrián Alcalá Méndez
INAI Commissioner, Mexico

In 2015, the "2030 Agenda" approved by the United Nations Organization presented 17 main Objectives, with 169 multidisciplinary goals that cover economic and social aspects: such as the elimination of poverty, actions to combat climate change, education, reduction of inequalities, and inclusion, as well as the restructuring of the design of societies, explicitly based on human rights.

Accelerating the progress of the mechanisms based on the Sustainable Development Goals (SDG) is essential to achieving the goals contemplated. In this sense, global efforts and international cooperation are key tools. The sustainable and inclusive economies that encourage investment and the political, technological, social, and financial proposals must be reconsidered effectively and with leadership to adapt these current instruments of change to the SDG.

Inequality within countries has caused a state of uncertainty and concern of a global nature because despite some positive signs towards combating it, —implementing a balance of income in some countries and preferential trade status that benefits developing countries— inequality persists.

The regulatory framework for the protection of personal data may be essential for the protection of human rights due to its interdependence by constituting itself as a fundamental right through which the scope of other rights is potentiated. This is in the understanding that their object includes the safeguarding of information that identifies or makes identifiable people, and a budget that allows these prerogatives to be attributed and individualized.

The human rights perspective constitutes an end and a starting point of the reference framework for well-being and sustainable development, so it is estimated that developing a protocol related to the validity of human rights will always provide valuable experiences

to those who implement it and that tend to the progressivity of the rights achieved and allow its constant expansion.

The Covid-19 pandemic brought serious consequences in terms of loss of life and economic development, which has significantly prevented progress towards compliance with the Sustainable Development Goals, making it more evident the inequalities that historically have caused damage to humanity, but above all, to the most vulnerable communities. It has also managed to put into perspective those abysmal differences in sectors such as the economic, social, and political, as well as the fragility of the safety nets that mean that these communities have to suffer the consequences of the health crisis.

Economic and social policies must acquire a universal character, paying particular attention to the needs of the most unprotected communities, which become more vulnerable. In this sense, it is necessary to provide legal certainty to all people who, due to circumstances arising from their environment, are unable to have access to the means required for the full recognition of their right to privacy and the protection of their personal data, since if they achieve full exercise of the same, could be translated into a fundamental weapon to reduce the gaps and guarantee that all individuals are treated with dignity and respect for their human rights.

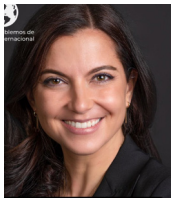
La desigualdad dentro de los países ha provocado un estado de incertidumbre y preocupación de carácter global. Ante tal situación, el marco normativo de protección de datos personales es ser esencial para la protección de los derechos humanos por su interdependencia, al constituirse como un derecho fundamental a través del cual se potencializa el alcance de otros derechos.

La perspectiva desde los derechos humanos constituye un fin y un punto de partida del marco de referencia para el bienestar y el desarrollo sustentable. La pandemia por Covid-19 trajo consigo consecuencias graves lo que ha impedido de manera significativa el constituir un avance hacia el cumplimiento de los Objetivos de Desarrollo Sostenible, evidenciando las desigualdades que históricamente han afectado a la humanidad.

Las políticas económicas y sociales deben adquirir un carácter de universalidad, prestando especial atención a las necesidades que presentan las comunidades más desprotegidas y que por ende se vuelven más vulnerables.

Mariana Salazar Albornoz

Member and Rapporteur on Privacy and Data Protection, Inter-American Juridical Committee, Organization of American States (OAS).
@msalazaralb



As recognized by the 2021 Sustainable Development Goals (SDG) Report, the global COVID-19 pandemic has halted and reversed decades of advancement in reaching the 17 SDG's by the 2030 deadline. The rise in the global extreme poverty rate, the increased

number of children who have fallen below the minimum reading proficiency level, the threatening of the livelihoods of 1.6 billion workers in the informal economy, the deepening of gender inequalities, the persistence of the climate crisis and the intensification of financial difficulties and inequalities within and among countries, are only some of the many challenges involved.

Data plays an essential role in the advancement of the 2030 Agenda. As stated in the Agenda itself, "*[q]uality, accessible, timely and reliable disaggregated data is needed to help with the measurement of progress*" of the SDG's. It is also "*key to decision making*", in the sense that it serves to engage stakeholders at all levels to advance evidence-based policies and programs to reach the most vulnerable and ensure that no one is left behind. The technological acceleration that came with the pandemic was accompanied also by an upsurge in innovative technologies and methods to collect, use and process data to monitor the SDGs.

While recognizing the urgent need to invest more in data, the 2021 SDG Report also emphasized the need to put in place, as a requisite for those innovative data collection methods, proper data governance methods to guard the privacy of individual information. To do so, adequate knowledge, dissemination, and compliance with relevant applicable international standards on privacy and data protection, by both public and private entities, is of essence.

The past few years have seen a significant proliferation of legal frameworks on privacy and data protection. Privacy laws are being adopted or updated at the national level in more and more countries each year. Businesses are increasingly putting in place policies to ensure responsible and ethical treatment of the data they collect. At the international level, the UN has adopted guidance notes and principles on data protection for achievement of the 2030 SDGs. Various regional organizations have adopted privacy regulations, including, notably, the European Union's General Data Protection Regulation, in force since 2018. At the inter-agency level, the Ibero-American Network adopted standards in 2017.

In order to reflect these legal developments, in 2021 the Organization of American States' (OAS) Inter-American Juridical Committee updated its *Principles on Privacy and Personal Data Protection*, with notes[4]. These Updated Principles are the result of extensive consultations held under my Rapporteurship with OAS Member States and international agencies. The 13 Principles were adopted by Member States, through the OAS General Assembly, in October 2021, and serve as a legislative and policy guide for States and businesses of the Americas that are in process of revising their privacy laws and policies. We hope that this regional framework contributes positively in our common endeavor of protecting privacy while collecting data, as a means to inform and advance the 2030 UN SDG Agenda.

Los datos juegan un papel esencial en el avance de la Agenda 2030 de las Naciones Unidas. Como se establece en la propia Agenda, "se necesitan datos desglosados de calidad, accesibles, oportunos y confiables para ayudar a medir el progreso" de los Objetivos de Desarrollo Sostenible.

[4] Available at: https://www.oas.org/en/sla/iajc/docs/CJI-RES_266_XCVIII-21_EN.pdf

Si bien se reconoce la necesidad urgente de invertir más en datos, el Informe ODS 2021, enfatizó la necesidad de implementar, como requisito para esos métodos innovadores de recopilación de datos, métodos adecuados de gobernanza de datos para proteger la privacidad de la información individual.

En 2021 el Comité Jurídico Interamericano de la Organización de los Estados Americanos (OEA) actualizó sus Principios sobre Privacidad y Protección de Datos Personales. Estos son el resultado de amplias consultas realizadas bajo mi Relatoría con los Estados Miembros de la OEA y organismos internacionales. Esperamos que este marco regional contribuya, positivamente en nuestro esfuerzo común de proteger el derecho a la privacidad mientras se recopilan datos, como un medio para informar y promover la Agenda 2030 de los ODS de la ONU.

Massimo Marelli

Head of the Data Protection Office
at the International Committee of the Red Cross.

The topic of today looks at humanitarian action, and at how the humanitarian sector itself has increasingly been using new technologies with a view to making its work more effective and efficient.

This is driven by a number of key factors such as:

• the famous blanket problem: pressure from donors to do more with less;

• a duty towards affected populations to do whatever we can to make our work have more impact and reach further, and to leverage technology in so far as this can enable us to do so;

• conflicts last longer (on average the 10 conflicts in which the ICRC has its most significant operations have been lasting approximately 40 years) with people increasingly relying on assistance in the longer term. Cash transfer programmes become useful tools, and these are often linked with the use of biometrics and the creation of digital identities. The use of blockchain is often suggested as relevant to support such programmes;

• conflict theatres become more volatile and difficult to read as you no longer have two armies lining up, one facing the other in bright colours helping you to understand who is who and where. We nowadays deal mainly with non-international armed conflicts, with factions often involved in shifting alliances, splinter groups, radicalised groups, and it is difficult to know who to speak to if you are trying to negotiate access and carry out a bilateral confidential dialogue (big data, AI and machine learning can help);

• with increasing challenges relating to access, physical proximity becomes increasingly challenging, leading us to look for new ways of complementing it with digital proximity (drones, messaging apps).

There are many implications involved in this exponentially augmented digital footprint of the humanitarian sector. Some of them bring into the heart of the discussion personal data protection and privacy.

For humanitarian organisations, like the ICRC, that have at the heart of their mandate the protection of and assistance to affected populations, protecting and treating personal data with respect means protecting and respecting affected populations. This means that, without calling it so, we have been applying data protection for a long time.

The complexity of the new technological landscape, however, makes it such that the humanitarian sector must also rely more and more on personal data protection, and its body of laws and tools, to ensure the protection of the rights and dignity of individuals when processing their data.

Personal data protection therefore becomes a tool for humanitarian organisations to apply the principle of 'do no harm' in a digital environment, and to keep the individual at the centre of a humanitarian response.

It all sounds good, but what does it mean in practice? For a few years now, we have been working with many experts in the field to create guidance, for example with the Handbook on Data Protection in Humanitarian Action[5]. The Handbook looks at the basic data protection principles contextualised in a humanitarian environment and at the declination of these principles in the use of certain specific technologies such as AI, biometric data, cash programmes, cloud, or other technology areas that are incredibly complex, such as digital identity.

Existen muchas implicaciones involucradas en la huella digital exponencialmente aumentada del sector humanitario. Algunos de ellos traen al centro de la discusión la protección de datos personales y la privacidad.

Para las organizaciones humanitarias, como la Cruz Roja, cuyo mandato principal es la protección y la asistencia a las poblaciones afectadas, el proteger y tratar los datos personales con respeto significa de igual manera el proteger y respetar a las poblaciones afectadas. La complejidad del nuevo panorama tecnológico hace que el sector humanitario también deba confiar cada vez más en la protección de datos personales, y en su cuerpo de leyes y herramientas para garantizar la protección de los derechos y la dignidad de las personas al procesar sus datos.

Desde hace algunos años, hemos estado trabajando con muchos expertos en el campo para crear una guía, el Manual sobre protección de datos en la acción humanitaria. Este Manual analiza los principios básicos de protección de datos contextualizados en un entorno humanitario y la relación de estos principios en el uso de ciertas tecnologías específicas como la IA, datos biométricos, programas en la nube y otras áreas que son increíblemente complejas.

[5] ICRC, 'Handbook on data protection in humanitarian action' (2nd edition). Available at: «https://www.icrc.org/en/data-protection-humanitarian-action-handbook».

Mila Romanoff

Privacy Specialist, Data Policy and Governance Lead

Data is essential in achieving the 2030 Agenda and its Sustainable Development Goals (SDGs). The UN Secretary-General High-Level Panel on Digital Cooperation issued the Roadmap with recommendations, calling for quality data access while also protecting the right to privacy. The UN Secretary-General Report "Our Common Agenda" noted the importance of trust. I believe that data protection and respect for data privacy may help ensure data is used properly for the public good. Data protection can be also key in enhancing and establishing trust in the value of data to benefit the global society.

Data Protection and Privacy is paramount across the UN. Many UN organizations have internal policies, guidelines and procedures on data protection —where IOM, UNHCR, WFP, UNICEF, ILO are only a few examples. In 2016, UN Global Pulse, a special initiative of the UN Secretary-General, co-led the establishment of the inter-agency working group– the UN Privacy Policy Group. Its primary objectives are to "(i) advance dialogue and information sharing on key issues related to data privacy and protection within the UN system; (ii) unite existing efforts on data privacy and protection; and (iii) develop a practical UN System-wide framework on data privacy and protection. Thanks to the efforts of this Group, the UN system organizations issued and adopted the UN Principles on Personal Data Protection and Privacy in 2018. The Principles set out a basic framework for processing "personal data" by, or on behalf of, the UN system organizations in carrying out their mandated activities. One of the important parts in the UN Principles is reference to non-personal sensitive data, acknowledging the need to protect data that is not directly identifiable. The Principles call for protecting data that may identify vulnerable groups of individuals.

In 2017, UN Global Pulse co-led the development of the Guidance Note on Big Data for the 2030 Agenda: Data Protection, Ethics and Privacy, which was adopted by the UN Sustainable Development Group. This was one of the first high level inter agency instruments on data protection that considered the challenges of data use for the public good. It looked at the importance of assessing both: the risks and the benefits of data use for the public good. Much earlier, Global Pulse developed an instrument the Risks, Harms and Benefits Assessment that introduced the same assessment approach, while also recognizing the importance of group harms, especially in sensitive humanitarian contexts and while affecting vulnerable populations. The notion of group harms in technology as well as the need for assessment of risks, harms and benefits is not a new concept, worked on by various stakeholders, yet it may be useful in evaluating the need and the possibility to use data for public good.

Data use is widespread. There were multiple examples when data was used to combat the COVID-19 pandemic, including for monitoring the spread of the virus, containing it, and beyond. However, its increased use raised concerns among privacy and data protection experts, both within and outside the UN system.

With UN entities noting the urgent need for guidance on the privacy-protected use of data, the UN Privacy Policy Group (UNPPG) developed the Joint Statement on Data Protection and Privacy in Response to COVID-19. The Statement was issued and endorsed by many UN organizations to reinforce the UN's commitment to using data and technology in a way that respects the right to privacy and other human rights. The goal of the Statement is to inform and guide the global response to COVID-19 across the UN system. It aligns with the UN Principles on Personal Data Protection and Privacy, as well as such key policy instruments as the UN Secretary-General's Call to Action for Human Rights and the UN Secretary-General's Data Strategy. The hope is that the Statement can serve as a precedent for using data to respond to future emergencies in a way that preserves fundamental human rights and freedoms.

As we look back, data protection has become important across many different sectors and certainly in the international public sector. This especially concerns the situations of humanitarian importance. There is no doubt that we need to use technology and data to benefit the people. My hope is that the many lessons learnt during the recent health pandemic will not be forgotten. Rather, the lessons will help the global society, the decision- and the policy-makers, create paths towards a sustainable, agile, privacy protective and responsible use of data that can not only benefit our social and economic well-being, but also save lives.

Los datos son esenciales para lograr la Agenda 2030 y el cumplimiento de los Objetivos de Desarrollo Sostenible (ODS). El Panel de Alto Nivel sobre Cooperación Digital del Secretario General de las Naciones Unidas emitió una hoja de ruta con recomendaciones, pidiendo acceso a datos de calidad y protegiendo al mismo tiempo el derecho a la privacidad.

En 2016, UN Global Pulse, una iniciativa especial del Secretario General de la ONU, codirigió el establecimiento del grupo de trabajo interinstitucional llamado el Grupo de Política de Privacidad de la ONU. En 2017, UN Global Pulse codirigió el desarrollo de una Nota sobre Big Data para la Agenda 2030: protección de datos, ética y privacidad, que fue adoptada por el Grupo de Desarrollo Sostenible de la ONU.

Así mismo, gracias a los esfuerzos de este Grupo, se emitieron y adoptaron los Principios de las Naciones Unidas sobre la privacidad y la protección de datos personales en 2018, y se desarrolló la Declaración Conjunta sobre Protección de Datos y Privacidad en Respuesta al COVID-19.

No hay duda de que necesitamos usar la tecnología y los datos para beneficiar a las personas.

Inclusive Policies: Poverty and marginalization sectors in the protection of personal data

Oscar Mauricio Guerra Ford

Executive Secretary of the National Transparency Platform, INAI Mexico. Former INAI Commissioner, Mexico.

Information and Communication Technologies (ICT) offer a range of advantages for the population, such as greater access to information and greater connectivity between people. However, these digital benefits are not having an equal impact on all social sectors since there is an imbalance, which we know now as the digital gap. This gap has become even more exposed due to the pandemic afflicting us worldwide, as people having internet access were able to remedy various social needs, including work and education.

According to the International Telecommunications Union (ITU), the United Nations specialized agency (UN), around 3.6 billion people do not have access to an internet network, representing almost half of the world's population.

It is worth mentioning that at first, it was considered that the digital gap was a consequence of underdevelopment and that with the popularization of technologies it would gradually disappear. However, this has not been the case since the gap persists despite the advances and variety of technologies and the growing Internet access.

These conditions represent a real challenge to safeguard the protection of personal data in a highly digital field since the flow of information and personal data in cyberspace has been increasing. The pandemic has amplified all aspects of digital transformation, reaching unprecedented levels in data sharing and data flows.

For this reason, it should be considered a priority for governments to incorporate inclusion criteria in the design and implementation of public policies, where the States can guarantee: that their actions are free of mechanisms that produce inequality between the members of their societies; establish necessary and appropriate modifications and adaptations that do not impose a disproportionate or undue burden; guarantee people

in vulnerable situations the enjoyment and exercise of human rights, such as the right to privacy and the right to protection of personal data; all under equal conditions.

From the Mexican experience, I would like to highlight the implementation of the SISAI 2.0 system linked to the National Transparency Platform, which is a system of requests to access information and protection of personal data, with which people can send notifications through text messages or WhatsApp about the status of the population's requirements. This project includes the development of a free mobile application through which requests and complaints can be generated, registered, and followed up via notifications.

The right to data protection is a right of all people and is closely related to autonomy and freedom; therefore, organizations and institutions that process personal data must ensure that complete information is provided under equal conditions to the holders so that they can exercise their right to informative self-determination.

Las Tecnologías de la Información y Comunicación ofrecen grandes ventajas para la población, tales como un mayor acceso a la información y una mayor conectividad entre las personas. Sin embargo, estos beneficios digitales no están impactando por igual en todos los sectores sociales, pues existe un latente desequilibrio, al que hoy en día conocemos como brecha digital, y el cual ha quedado aún más expuesto derivado de la contingencia sanitaria que nos aqueja mundialmente; a través de este suceso, se identificó la importancia de contar con acceso a internet para poder subsanar diversas necesidades sociales, incluyendo el trabajo y la educación.

El derecho a la protección de datos es un derecho de todas las personas y está íntimamente relacionado con la autonomía y la libertad, por ello, las organizaciones e instituciones que realicen un tratamiento de datos personales están obligadas a garantizar que se proporcione en igualdad de condiciones y con información completa a las y los titulares para que puedan ejercer su derecho a la autodeterminación informativa.

Fredesvinda Montes

Senior Financial Specialist, Finance, Competitiveness & Innovation at the World Bank

Good morning everyone, fellow panelists, distinguished members of the Global Privacy Assembly and experts in the subject connected from different World regions. Let me thank INAI for inviting me to this panel which is very close to the World Bank objectives of poverty alleviation shared prosperity and economic growth.

Most of the work that we conduct on Data Protection and Privacy at the World Bank's Financial Competitiveness and Innovation Global Practice focuses on access to digital financial services. Traditionally, we have been engaged in supporting the development of data protection frameworks as complementary rules to the existing financial sector regulation to build TRUST in areas that required personal information data sharing to allow for

more access financial services. These individuals include unserved which fall under the category of vulnerable population underserved which can also include women, youth and migrants.

Since 2002, a great part of our work involved balancing credit information data sharing and data protection. This work resulted in the General Principles for Credit Reporting issued by International Committee on Credit Reporting (ICCR) chaired by the WB which includes 5 principles. 4 of those principles relate to data protection (data quality, data security, consumer rights and cross-border data flows). General Principles on Credit Reporting.

As the provision of digital financial services made its way, a broader scope of participants and types of data was required, and the World Bank paid particular attention to data protection as a subset of consumer protection framework for financial services. Good Practices of Financial Consumer Protection.

In collaboration with the Global Partnership for financial inclusion of the G20, the World Bank developed research studies and policy briefs on the use of alternative data to build credit scores with the objective of allowing additional individuals to proof their creditworthiness. We also worked closely with the Financial Action Task Force on the development of a framework for Digital ID which involves collection of personal information including biometric data. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf.

In addition, we work very closely with several government agencies in the development of Open Banking/open finance schemes which aim also at enabling a larger group of individuals access digital financial services through the implementation of the right to data portability. In this context, a recent paper on consent mechanisms for open banking aims at solving the conundrum around the traditional consent based on forms to a more practical way of providing and revoking consent by data subjects through dedicated apps providing more control to data subjects over their data.

Finally, under the Financial Stability Board, developing guidelines and roadmaps to enable cross-border payments which includes Building Block 6 on data frameworks and Building Block 8 on Digital ID that looks into the implications of personal information data sharing and data protection safeguards. https://www.fsb.org/2021/10/fsb-sets-out-progress-on-cross-border-payments-roadmap-and-publishes-targets-for-enhancing-cross-border-payments/.

All these initiatives translate in a deep analysis at country level but also into policy dialogue with relevant international organizations to move forward the financial sector agenda while also taking into consideration the need to protect data subjects from unauthorized access, misuse of data and unfair discrimination to all data subjects including in particular underserved and unserved groups.

La mayor parte del trabajo que llevamos a cabo sobre protección de datos y privacidad en la Práctica Global de Innovación y Competitividad Financiera del Banco Mundial se centra en el acceso a los servicios financieros digitales.

Por mencionar algunas de las inciativas que realizamos, desde 2002, una gran parte de nuestro trabajo implicó equilibrar el intercambio de datos de información crediticia y la protección de datos personales, por lo que en colaboración con la Alianza Global para la Inclusión Financiera del G20, desarrollamos estudios de investigación y resúmenes de políticas sobre el uso de datos alternativos para generar calificaciones crediticias. Además, trabajamos muy de cerca con agencias gubernamentales en el desarrollo de esquemas de banca abierta/finanzas abiertas.

Estas iniciativas se traducen en un análisis profundo a nivel de país, pero también en un diálogo de políticas con las organizaciones internacionales para hacer avanzar la agenda del sector financiero, al mismo tiempo que se tiene en cuenta la necesidad de proteger a los interesados del acceso no autorizado, y el uso indebido de los datos.

Gabriela Zanfir-Fortuna

Vice President, Global Privacy Future of Privacy Forum.
@gabrielazanfir

A plea to start leveraging the principle of fairness

It is becoming more urgent to tackle discrimination, negative effects, and power imbalances when it comes to collecting, using, and sharing personal data and its impact on vulnerable and marginalized people. This panel organized by INAI for GPA 2021 kicked off an essential global conversation about ways in which data protection law can be leveraged to address these problems.

One underexplored solution is to leverage the principle of fairness in data protection law. This principle is clearly provided in European Union's legal system for the protection of persons with regard to the processing of their personal data, from the text of Article 8 of the Charter of Fundamental Rights to the text of the General Data Protection Regulation (GDPR) in Article 5. However, to date it has been interpreted and applied in a limited way by supervisory authorities in Europe. For instance, the European Data Protection Board (EDPB) wrote in its Transparency Guidelines that fairness requires data controllers "to always consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing". Processing personal data fairly should mean more than this in today's data heavy society and it should be leveraged at least to protect vulnerable and marginalized people from discrimination and unfair or harmful effects.

For instance, while Brazil's LGPD does not provide for a principle of fairness per se, it does include a general rule that all data processing activities must observe "good faith" (Article 6) as a ground for several principles, including "non-discrimination". The latter is legally defined as the "impossibility of processing data for discriminatory, unlawful or abusive purposes" (Principle IX under Article 6). Other jurisdictions, like Japan, are molding this principle to their own legal culture. Japan's APPI provides as a rule the "proper handling" of personal information (Article 1). It also requires that personal information should be handled "under the vision of respecting the personality of an individual" (Article 3). Addi-

tionally, it provides in Article 16 that the business operators should not utilize personal information using a method that has the possibility of fomenting or prompting an unlawful or unfair act". Such provisions can add a substantial protection to vulnerable and marginalized individuals with regard to how personal data about them is being collected and used.

After this GPA 2021 panel, one of my co-panelists and the co-director of the Brussels Privacy Hub, Gianclaudio Malgieri, extended an invitation for our two institutions to found the International Observatory of Vulnerable People in Data Protection —VULNERA, which we are ready to launch on November 15, 2021—. The panel was just the beginning of a very fruitful international conversation on this topic.

Cada vez es más urgente abordar la discriminación, los efectos negativos y los desequilibrios de poder cuando se trata de recopilar, usar y compartir datos personales y su impacto en las personas vulnerables y marginadas.

Una solución poco explorada es aprovechar el principio de equidad en la ley de protección de datos. Este principio está claramente previsto en la Unión Europea en lo que respecta al tratamiento de datos personales, del artículo 8 de la Carta de los Derechos Fundamentales, y en el Reglamento General de Protección de Datos (GDPR) Europeo en su Artículo 5. Sin embargo, hasta la fecha ha sido interpretado y aplicado por las autoridades supervisoras en Europa.

Después de este panel de GPA 2021, uno de mis co-panelistas y codirector del Centro de Privacidad de Bruselas, Gianclaudio Malgieri, extendió una invitación para que nuestras dos instituciones fundaran el Observatorio Internacional de Personas Vulnerables en Protección de Datos —VULNERA, que lanzamos el 15 de noviembre de 2021—. Esto solo fue el comienzo de una conversación internacional muy fructífera sobre este tema.

Gianclaudio Malgieri

Associate Professor of Law and Technology at the EDHEC Business School in Lille (France). He is Co-Director of the Brussels Privacy Hub; Guest Professor at the Free University of Brussels (VUB); Editorial Board Member of Computer Law and Security Review; and External Expert of the European Commission (Research Executive Agency).

Inclusive data protection: the issue of vulnerable data subjects

In the last decade, more and more scholars and policymakers have considered privacy and data protection law as a promising field to address and mitigate human vulnerabilities, especially considering the increasing power imbalance between Big Techs and end-users of digital platforms.

Defining vulnerable data subjects is not a simple task: some vulnerabilities are based on historical marginalisation of groups (e.g., immigrants, ethnic minorities, racial minorities, LGBTQIA+ people); other forms of vulnerabilities are based on hierarchical or institutional asymmetries (e.g., employees are vulnerable in the relationship with their employer;

suspects or detainees are vulnerable in the relationship with law enforcement authorities); other vulnerabilities are based on socio-economic conditions of the data subject, on her age or disability, or even on temporary and induced weaknesses (e.g., online consumers whose cognitive biases are exploited by digital platforms).

In the EU GDPR, there is no clear definition of vulnerable data subjects, but just a slight reference to children as vulnerable data subjects. However, the European Data Protection Board often refers to vulnerable people, mentioning especially children, workers, and people in a condition of power imbalance. In addition, the GDPR is risk-based: the data protection measures should be proportional to the level of risk that the data processing brings to the fundamental rights and freedoms of data subjects. Accordingly, a mature definition of "vulnerable data subjects" in the EU should refer to the level of risks for data subjects' fundamental rights and freedoms. In other terms, vulnerable data subjects are those in a condition of higher risks for their fundamental rights and freedoms. Such a particular condition is always contextual and layered, but it can be permanent or transient, structural or relational.

But how can data protection mitigate human vulnerabilities? It depends on what kinds of risks we want to address. There are at least two aspects that data protection could consider. The first is the data subjects' difficulty understanding data protection policies, their risks and rights, and providing free and informed consent. The second aspect concerns risks to other fundamental rights when personal data are processed, especially discrimination, mental manipulation, and stigmatisation.

The first vulnerability aspect is evident in the case of children, the elderly, and people with cognitive limitations. Other examples can be workers who are incapable of refusing consent to their employers; or digital consumers who are in a situation of "lock in" and are, thus, incapable of denying consent when Big Techs ask them to share even the most sensitive personal data. In this case, data protection law can help, e.g., by imposing data controllers to reach higher standards of transparency and understandability, but also by limiting the possibility of consent requests in situations of a significant power imbalance between the data controller and the data subject.

The second vulnerability aspect is more complex. It is more difficult to measure, analyse and mitigate the impact of data processing on "other fundamental rights". However, the Data Protection Impact Assessments should be used for this goal. Data Protection Agencies should release specific guidelines for data controllers. These guidelines should indicate how to face the particular situation of data subjects' vulnerability (e.g., children, employees, social and ethnic minorities, digital consumers, etc.) and prevent or mitigate risks to their fundamental rights and freedoms (e.g., discrimination, stigmatisation, manipulation, etc.).

En la última década, cada vez más académicos y legisladores han considerado la ley de privacidad y protección de datos como un campo prometedor para abordar y mitigar las vulnerabilidades humanas, especialmente considerando el creciente desequilibrio de poder entre las grandes tecnologías y los usuarios de las plataformas digitales.

Definir sujetos de datos vulnerables no es una tarea sencilla: algunas vulnerabilidades se basan en la marginación histórica de grupos; otras en asimetrías jerárquicas o institucionales; otras en las condiciones socioeconómicas del interesado, en su edad o discapacidad, o incluso en debilidades temporales e inducidas.

Pero, ¿cómo puede la protección de datos mitigar las vulnerabilidades humanas? Depende de qué tipo de riesgos queramos abordar. Hay al menos dos aspectos que la protección de datos podría considerar. El primero es la dificultad de los interesados para comprender las políticas de protección de datos, sus riesgos y derechos, y prestar su consentimiento libre e informado. Y el segundo aspecto se refiere a los riesgos relacionados a otros derechos fundamentales cuando se tratan datos personales, en especial la discriminación, la manipulación mental y la estigmatización.

Valeria Milanes

Executive Director Asociación por los Derechos Civiles, Argentina

As part of our work in ADC (Asociación por los Derechos Civiles, Argentina) on technology and fundamental rights, we have analyzed diverse phenomena. We have progressed from the first stage of general understanding to the second stage of learning about technology's power on groups in vulnerable situations, such as people with disabilities, LGBTQ people, women, children, and adolescents.

This journey has allowed us to verify that when we are in front of groups in vulnerable situations, we cannot think about the technological issue, or issues of personal data of poor and marginalized sectors, without understanding the context in which this situation is generated and developed considering both intersectional and structural aspects. In this sense, I will emphasize elements that characterize poverty and structural inequality in Latin America and the Caribbean, which have been studied for a long time and which are very well reflected in the regional human development report 2021 published in June prepared by the United Nations Development Program entitled "Trapped: High inequality and low growth in Latin America and the Caribbean".

The report characterizes one of the world's most unequal and violent regions and refers to three reasons. One is the concentration of power, two is violence in all its forms, political, criminal, and social, and three the social protection systems that do not work well.

I will focus on the concentration of economic and political power, which means the depression of power in the hands of a few companies who defend the private interest. The report recognizes that monopoly power and corporate political power are two sides of the same coin, since monopoly rents translate into political power, which in turn increases monopoly power creating a virtual cycle that in American markets tend to be dominated by a small number of giant companies providing cell phone services, internet services, microfinance services, among others. I highlight the vast amount of personal data originating from these universal services. The political power of these firms distorts political power beyond the market level, including, for example, fiscal distortions, as the report also highlights.

As a consequence of the above, the report also reflects on the effectiveness of competition laws and agencies which lack the necessary powers to investigate or contain the situation through adequate fines or sanctions, adding that most of these offices are understaffed in terms of quantity and expertise of their staff. It should be added that the report's description of the characteristics of competition authorities also applies to most of the personal data protection authorities in the region.

Why do I bring these highlights?

The Latin American and Caribbean region has many challenges in adopting higher standard personal data protection regulations and terms of implementation and enforcement of those relations. There are social aid policies set as a palliative of the situation of poverty -though not overcoming it- for which all personal data, in many cases sensitive data, must be given imperceptibly to governments.

We cannot think about how to settle this enormous depth in the personal data protection systems at the local and regional level, nor begin to consider how best to protect the personal life of people living in poverty and marginalization without thinking from the very outset issues of competition: The concentration of political and economic power that is so deeply rooted in this region and have such adverse effects in consequences to tackle inequality.

I am aware of the particular interest of the GPA in fostering conversations between data protection and competition authorities. We, from civil society, will do our best to push these conversations to understand these interactions and their consequences better and hopefully promote proper actions that most benefit these sectors that live in poverty and are marginalized.

Como parte de nuestro trabajo en la Asociación por los Derechos Civiles en Argentina sobre tecnología y derechos fundamentales, hemos analizado diversos fenómenos. Hemos pasado de la primera etapa de comprensión general a la segunda etapa de aprendizaje sobre el poder de la tecnología en grupos en situación de vulnerabilidad.

Este recorrido nos ha permitido comprobar que cuando estamos frente a grupos en situación de vulnerabilidad, no podemos pensar en el tema tecnológico, ni en temas de datos personales, sino que debemos entender el contexto en el que se genera y desarrolla esta situación, considerando tanto aspectos interseccionales como estructurales.

Reconozco el interés de la GPA en fomentar conversaciones entre las autoridades de protección de datos y de competencia. Nosotros, desde la sociedad civil, haremos todo lo posible para impulsar estas conversaciones para comprender mejor estas interacciones y sus consecuencias y, con suerte, promover acciones adecuadas que beneficien más a estos sectores que viven marginados y en pobreza.

Regional cooperation in matters of privacy and personal data

Francisco Javier Acuña Llamas

INAI Commissioner, Mexico

Data flows brings together a series of benefits for national communities, such as the promotion of peace and democracy, the promotion of technical progress and growth, the economic interdependence of nations, the internationalization of companies and the specialization of national activities.

The health emergency caused by COVID-19 has confirmed to us that data flows are critical to the world economy, allowing both economic responses (for example, data exchange for medical research, automated monitoring, control of production of vaccines, and the adoption of digital services for business continuity), and social responses (for example, family video calls, contact tracing, streaming content for entertainment, and online shopping). Therefore, we are in a reality where data flows will continue to increase as more countries and sectors adopt and join the digital transformation.

In this sense, the technological revolution of electronics and the progress of telecommunications have allowed the development of international information flows to be transnational, making it easier for commercial activities, data processing, and personal data.

The regulation on the cross-border flow of personal data must be focused on achieving a positive balance. On the one hand, companies need to obtain information, and the easier they are to collect data, as well as for its storage, transfer, analysis, and trade, the greater its economic benefits. On the other hand, recent incidents of private information being shared or exposed have increased public awareness of the risks they pose to personal data stored online. These data privacy concerns may become more urgent with the expansion of the amount of information online that organizations access and collect and the level of global data flows.

It has made it more than clear to us the economic and social benefits that international transfers of personal data have today. However, the question that persists is not why? But how to carry them out while protecting the rights of data owners when their information is sent to other countries?

Today, the cross-border movement or transfer of personal data is unstoppable, but there are no global rules governing the use or protection of this data. Reconciling the different perspectives and approaches on the matter and seeking to establish a global interoperability system that is neither discriminatory between other national data protection systems nor restrictive in the commercial sphere is not a minor task since it requires the consideration of multiple edges that must be exposed and studied with the objective of being able to guarantee an appropriate level of protection for the people concerned by the information, but also to avoid the adoption of unnecessary barriers to the free movement of such information, with its harmful effects for a global and interconnected economy.

El flujo de datos, trae consigo una serie de beneficios para las colectividades nacionales. La regulación sobre el flujo trasfronterizo de datos personales debe estar enfocada en alcanzar un balance positivo entre los intereses que lo anteponen. Por un lado, las empresas presentan una necesidad de obtener información y entre más facilidad tengan para la recopilación de los datos, así como para su almacenamiento, transferencia, análisis y comercio, mayores serán sus beneficios económicos, siempre y cuando se dé un uso adecuado a los datos obtenidos.

Por otro lado, los incidentes recientes de información privada compartida o expuesta han aumentado la conciencia pública sobre los riesgos que representan para los datos personales almacenados en línea. Estas preocupaciones sobre la privacidad de los datos pueden volverse más urgentes con la expansión de la cantidad de información en línea a la que las organizaciones acceden y recopilan, y el nivel de los flujos de datos globales.

Conciliar las diferentes perspectivas y enfoques en la materia y buscar establecer un sistema de interoperabilidad mundial no discriminatoria entre diferentes sistemas nacionales de protección de datos, ni restrictiva en el ámbito comercial, no es un trabajo menor pero puede realizarse.

CLARISSE

Caroline Louveaux

Chief Privacy Officer at Mastercard

Understanding the importance of global data flows

Cross-border data flows are the lifeblood of our global digital economy. Just take the retail data ecosystem, it heavily relies on global data flows at every step:

- To process your payments
- To protect you against fraud
- To provide you with 24/7 customer support
- To ensure business continuity

• To ship the goods you have bought online

• To provide you with the loyalty rewards you have signed up to

And the list goes on

What this means for the global payments system

Mastercard is a global payments and technology company. We transmit and handle the transaction data of millions of cardholders and merchants every day. For our payment system to work properly, transaction data need to flow freely across borders.

We are in a unique position to monitor and detect fraud thanks to transaction data from a multitude of financial institutions. Indeed, to identify patterns of fraud, we need to be able to collect and share payment data from across the globe. Because more transactions give us better predictions, so that we can connect the dots and detect potentially fraudulent transactions in real time.

Key challenges

Today, while laws and regulations are quickly emerging on how data can be collected, used, shared and stored, we face fragmentation of standards across the globe. Furthermore, restrictions on cross-border data transfers and data localization requirements are on the rise, forcing companies to process and/or store data "on soil".

This results in bad outcomes for everyone; it creates complexity and higher operational expenses for companies, to the detriment of smaller enterprises. It also adversely impacts safety and security and ultimately leads to an increase in costs and reduction in choice and quality for consumers.

The way forward

The good news is that we can have free flows of data while fully protecting data end-to end. To get there, both the public and private sector must demonstrate accountability when handling data. What do we mean? This requires protecting data with high privacy and security safeguards ("the what"), wherever the data goes ("the where") and implementing tools to ensure these controls are working effectively ("the how").

For the industry, accountable privacy programs and data transfer solutions can take many forms and shapes. Whether relying on Binding Corporate Rules (BCRs), APEC Cross-Border Privacy Rules (CBPRs) or Standard Contractual Clauses (SCCs), what's important is protecting the data with high privacy and security controls across your organization. Ensuring effective protection includes:

• Securing executive buy in and oversight.

• Implementing policies, standards and procedures about do's and don'ts.

• Having a network of privacy and data protection officers globally.

• Training the organization about privacy and data protection commitments.

• Monitoring compliance and having a mechanism in place to remedy any gaps, to respond to individuals' complaints and offer redress and compensation.

It's time to double down on dialogue and cooperation among policymakers, industry, academics and civil society across jurisdictions to develop pragmatic solutions to facilitate trusted data flows.

MasterCard es una empresa global de pagos y tecnología. Transmitimos y manejamos los datos de transacciones de millones de titulares de tarjetas y comerciantes todos los días. Para que nuestro sistema de pago funcione correctamente, los datos de las transacciones deben fluir libremente a través de las fronteras.

En la actualidad, surgen rápidamente leyes y reglamentos sobre cómo se pueden recopilar, utilizar, compartir y almacenar los datos, nos enfrentamos a la fragmentación de los estándares en todo el mundo. Además, las restricciones a las transferencias de datos transfronterizas y los requisitos de localización de datos van en aumento, lo que obliga a las empresas a procesar y/o almacenar datos "en el suelo".

Esto crea complejidad y mayores gastos operativos para las empresas. La buena noticia es que podemos tener flujos de datos libres mientras protegemos completamente los datos de principio a fin. Para llegar allí, tanto el sector público como el privado deben demostrar responsabilidad al manejar los datos.

Clarisse Girot

Senior Fellow, Asian Business Law Institute (Singapore)

Head of the Data Governance and Privacy Unit at OECD

Thank you for the invitation to provide thoughts in this crucial conversation about the regulations of cross-border data transfers, arguably one of the most complex issues which policymakers in the digital economy are facing today.

I would like to take this opportunity to share some personal thoughts that came to me upon realizing that I entered the world of personal data protection exactly 20 years ago, during which issues relating to data transfers have always taken a considerable amount of time and reflection. Hopefully these reflections can contribute to putting today's conversations into perspective. I will share three.

My first observation pertains to the globalization of policy and rulemaking in data protection and data flows, alongside the globalization of technologies and data flows themselves. This irreversible trend has a dramatic impact on all the stakeholders involved in these discussions, and particularly for the members of the Global Privacy Assembly. What was for a very long time largely a transatlantic conversation between the EU and the US, the epicenter of policy and rulemaking in data flows, has radically changed. From my home office in Singapore, just like others in Bangkok, Hong Kong, Tokyo, we see a sea change happening, in the Asia Pacific region and beyond, as more jurisdictions are passing new data protection laws in the region, and two "giants" are on everybody's minds here: in 2021, China released its Personal Information Protection Law, and India could finally adopt its own Data Protection Act in 2022 (although cautious optimism should prevail). It is striking that virtually all of

these new laws now have extraterritorial effect and include data transfer provisions, leading many jurisdictions to adopt data transfer policies, tools, mechanisms, and arrangements adapted to the region. Surely we are far from having taken the full measure of the changes underway. Policymakers are looking at the same issues around the globe, but increasingly often through different lenses, and against different backdrops. In particular, the philosophy of the most recent data transfer regulations can be very different from that which presided over those of the first data protection laws: today we speak as much of "data sovereignty" and national security as of the protection of the fundamental rights of individuals that flows with their data. Indeed, the privacy landscape is more fragmented than before, compliance obligations have become harder to meet in a cross-border context, regulatory risks have significantly risen. But it is not all gloom and doom. On the other hand, we can also look at some of these complexities as the price of success: a sign that people's privacy expectations are on the rise, as more data protection laws are being passed. Alongside these regulatory developments, we now have a broad community of privacy regulators, a broad community of privacy professionals globally. More academics are coming into this space, data protection curriculums are developing at universities and in schools, civil society groups have grown in privacy expertise and public exposure. Privacy can be a powerful competitive advantage, a global privacy tech market is developing... The privacy challenges we face are very real, but the sophistication of the ecosystem that is being put in place around privacy should encourage us to be optimistic.

My second comment is that we must however guard ourselves against the "technicization" and "compliancification" of privacy as more laws and regulations are passed in this field. The fact that the accumulation of elaborate legislations has contributed to turning data protection and privacy into a complex compliance field globally should not end up obstructing the purpose of data transfer regulations. Cross-border flows have been regulated historically because the protection of our rights and freedoms is at stake when bits and pieces of our personalities leave the protection which they enjoy in our home jurisdiction; in fact this myriad of small data elements, taken individually or aggregated together, say a lot about ourselves, our families, the life of businesses, their projects, their operations, their employees, the functioning of our democracies, the state of our communities, and the movements of our societies. All the underlying challenges cannot be left to solve by an elaborate construct of checkboxes which one cannot not tick, consent mechanisms, privacy policies which no one reads, and other tools presented as automatically "GDPR or CPPA compliant", which they are not, however expensive they are. It matters to take a step back and reflect on "why" we have these regulations in the first place instead of only focusing on the "how". We need to take a holistic approach to data transfers and avoid the risk to transform these topics into excessively technical subjects reserved for specialists. For regulators and policymakers, this risk can be avoided in particular through building commonalities and common understandings between jurisdictions, and trying to find convergence in everything they do. This is the spirit of the work which we have been doing on cross-border data flows in Asia-Pacific, at the Asian Business Law Institute.

A third and last lesson learnt is that it would be wrong —and in fact, maybe even presumptuous— to argue that the complexities we face today are immeasurably greater than those

of the past, and that the questions that arise today might not be answered. I took up my first privacy job at CNIL on September 3rd, 2001, as we were then just in the home stretch of the organization of the Global Privacy Assembly conference (then ICDPPC), on September 24th and 25th, 2001. Among the topics on the program were cross-border data flows and the new standard contractual clauses that the European Commission had adopted in June 2001, and the ongoing review of the (since then two times defunct!) EU Safe Harbor decision. What's new, you could say! And then, just one week later, the Twin Towers fell. This dramatic event turned the world upside down, including our data protection world. In just a few weeks, a long series of extraterritorial laws including the Patriot Act and unprecedented government actions began being passed in the United States and all around the world, in reaction to this dreadful attack. The US Aviation and Transportation Security Act in November 2001 introduced a requirement that airlines operating passenger flights to the US provide the US authorities upon request with electronic access to passenger name record data (PNR), whose far reach was challenged in the EU. The agreement which was signed between the EU and the US in 2004, was struck down by the European Court of Justice in 2006. The trend became entrenched: FATCA, Sarbanes-Oxley, FCPA, SWIFT…

All this may sound highly familiar in the post Schrems II context! But 20 years back, we were having these difficult conversations about data flows and how to strike the right balance between competing public policy interests through extraterritorial laws, complex data transfer regulations and arrangements. Let us not despair of finding solutions to the current problems, however complex they may be. Far from negating the complexity of current challenges, we must remember that we solved others, which also seemed insurmountable in the past. In truth, the resolution of difficulties is directly indexed to the willingness of the stakeholders concerned to reach an agreement that takes into account the interests of the other. No technical measure can compensate for lack of trust. But once we have trust, technical implementation measures will follow.

Quisiera aprovechar esta oportunidad para compartir algunas ideas que me surgieron al darme cuenta de que entré en el mundo de la protección de datos personales hace exactamente 20 años, durante los cuales los temas relacionados con las transferencias de datos siempre han requerido una cantidad considerable de tiempo y reflexión. Espero que estas reflexiones puedan contribuir a poner en perspectiva las conversaciones de hoy. Me centraré en tres.

Mi primera observación se refiere a la globalización de las políticas y la elaboración de normas en materia de protección y flujos de datos, junto con la globalización de las tecnologías y los propios flujos de datos. Esta tendencia irreversible tiene un impacto dramático en todas las partes interesadas involucradas en estas discusiones, y en particular para los miembros de la Asamblea Global de Privacidad.

Mi segundo comentario es que debemos cuidarnos de la "tecnificación" y el "cumplimiento" de la privacidad a medida que se aprueban más leyes y reglamentos en este campo. El hecho de que la acumulación de legislaciones elaboradas haya contribuido a

convertir la protección de datos y la privacidad en un campo de cumplimiento complejo a nivel mundial no debería terminar entorpeciendo el propósito de las regulaciones de transferencia de datos.

Una tercera y última lección aprendida es que sería erróneo —y tal vez incluso presuntuoso— argumentar que las complejidades a las que nos enfrentamos hoy son inconmensurablemente mayores que las del pasado, y que las preguntas que surgen hoy podrían no tener respuesta.

Javier López González

Senior Economist, Trade and Agriculture Directorate of the OECD.

Mapping commonalities in regulatory approaches to cross-border data transfers[6]

Today's digitised and globally interconnected world is underpinned by the movement of data across borders. They, enable international social interactions; they help address global challenges ranging from energy, to mobility, through to health; and they enable the coordination of production along global supply chains and allow firms, especially smaller ones, to access global markets. In short, they are the lifeblood of our modern day social and economic interactions.

However, these cross border data flows also raise or amplify concerns across a number of policy areas including privacy protection, digital security, intellectual property protection, trade, competition and industrial policy. These concerns have led to the adoption of a growing number of rules that condition the movement of data across borders or that mandate that data is stored or processed in specific locations.

There are many reasons behind this rising regulation, which reflects a range of objectives, including privacy and data protection; regulatory control or audit; national security; digital security and digital industrial policy. And although there are legitimate reasons for diversity in regulation, often reflecting different cultural and legal backgrounds, the resulting landscape that underpins cross-border data flows is becoming increasingly complex. The emerging patchwork of rules and regulations is making it difficult not only to effectively enforce public policy goals such as privacy and data protection across different jurisdictions, but also for firms to operate across markets, affecting their ability to internationalise and benefit from operating on a global scale.

Against this backdrop, Governments have turned to a range of regulatory and policy 'instruments' to enable the movement of data across borders while ensuring that, upon crossing a border, data is granted the desired degree of protection or oversight. This has come to be known as Data Free Flows with Trust.

---

[6] This draws on work carried out at the OECD summarised in the following analytical report:
Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers", OECD Trade Policy Papers, No. 248, OECD Publishing, Paris, https://doi.org/10.1787/ca9f974e-en.
The views expressed are those of the author and do not represent the views of the organisation or its member states.

These include regulatory and policy instruments such as:

• **Unilateral mechanisms** such as the use of contracts or adequacy decisions as well as the accountability principle.

• **Plurilateral arrangements** which are largely developed in the context of privacy and data protection and include the OECD privacy guidelines, Convention 108+ and APEC CBPR.

• **Trade and digital economy agreements** with provisions on data flows (and privacy and personal data protections) such as CPTPP, USMCA or the EU-UK TCA.

• Alongside these efforts, **standards and technology driven initiatives**, referring technological solutions such as the use of privacy enchancing technologies or to ISO-IEC standards.

Recent work has shown that there is no single mechanism to enable *data free flows with trust*. Governments pursue different, or even multiple and complementary, approaches. However, by mapping commonalities in regulatory approaches to cross-border data transfers, we can identify how countries create "trusted" environments enabling cross-border data flows.

The work shows that there are a number of elements that can help international discussions:

• There are a range of **commonalities** in goals across different approaches. For example, the dual goal of enabling flows while maintaining trust is common across unilateral mechanisms, inter governmental arrangements and trade agreements. There are also commonalities within the approaches themselves. For instance, the use of contract is common as a means for transferring data abroad in the context of unilateral mechanisms.

• There are also some apparent **elements of convergence**. For example, there is convergence towards common principles in privacy and data protection or towards common and binding language in trade agreements.

• Finally, there are a number of emerging **complementarities** between existing instruments. For example, unilateral mechanisms are discussed in inter-governmental arrangements and trade agreements increasingly reference inter-governmental arrangements.

Together, these can be seen as indicating the emergence of an international architecture, or architectures, aimed at reaping the benefits of data flows while enabling governments to meet other legitimate public policy objectives.

While it remains the prerogative of governments to establish the mix of instruments or mechanisms that best serve their policy interests and objectives, greater understanding, discussion and agreement on these instruments can be conducive to greater overall confidence and "trust" in the environment that underpins the global flow of data and that supports a growing share of our economies and societies.

El mundo de hoy, digitalizado e interconectado globalmente, está respaldado por el movimiento de datos a través de las fronteras. Los datos son el elemento vital de nues-

tras interacciones sociales y económicas modernas. Sin embargo, estos flujos de datos transfronterizos también plantean o amplifican las preocupaciones y han llevado a la adopción de un número creciente de reglas que condicionan el movimiento de datos a través de las fronteras o que exigen que los datos se almacenen o procesen en ubicaciones específicas.

El abanico de reglas y regulaciones está dificultando no solo hacer cumplir de manera efectiva los objetivos de política pública, como la privacidad y la protección de datos en diferentes jurisdicciones, sino también que las empresas operen en todos los mercados, lo que afecta su capacidad para internacionalizarse y beneficiarse de operar a escala global.

Trabajos recientes han demostrado que no existe un mecanismo único para permitir flujos libres de datos con confianza. Sin embargo, los gobierno siguen intentando establecer instrumentos y mecanismos que mejor sirvan a sus intereses y objetivos para lograr una mayor "confianza" que sustente el flujo global de datos.

Yeong Zee Kin

Assistant Chief Executive (Data Innovation and Protection Group), Infocom Media Development Authority, Singapore (IMDA) and Deputy Commissioner, Personal Data Protection Commission (PDPC)

I am pleased to have this opportunity to share Singapore's views on cross border data flows and data protection, on this occasion of the Global Privacy Assembly 2021. The ability to transfer personal data across borders is fundamental and essential in a digital economy. I will be sharing about the ASEAN experience in developing Model Contractual Clauses (MCCs) to provide a baseline standard of protection across all its member states.

Regional Convergence: ASEAN Initiatives

1. ASEAN has a diverse data protection landscape. The approach towards data protection and privacy developments varies from country to country, with countries in different stages of maturity. Member states like Malaysia, Philippines, Thailand and Singapore have enacted general data protection laws; while others like Brunei and Indonesia are working on draft data protection bills. The rest of ASEAN rely on sectoral regulations for the protection of personal data. This lack of harmonisation is not unique to ASEAN and can pose compliance challenges for businesses operating within ASEAN. Given such varied approaches, how can data transfers be facilitated while ensuring comparable standards of protection?

2. Despite this complexity, ASEAN Member States have banded together in recognition of the importance of facilitating free but safe data flows to support the growing digital economy in ASEAN.

3. Contracts are an effective baseline mechanism to ensure a comparable standard of protection within an area of diversity. In ASEAN, we have the ASEAN MCCs, a set of ready-to-use and flexible terms and conditions that companies may include in binding legal agreements between businesses transferring personal data across borders. These MCCs

translate the ASEAN Framework on Personal Data Protection into contractual obligations, that businesses can hold their partners to in order to ensure a level of protection that is aligned with global best practices to ensure accountability. The ASEAN Data Management Framework supplements the MCCs by providing guidance on data governance and data protection safeguards throughout the data lifecycle.

4. Collectively, these are meant to be used across ASEAN Member States, and help to reduce lengthy contractual negotiations between businesses transferring data across ASEAN Member States.

Global Harmonisation: Certification Systems

5. In the longer term, the use of certifications as a mechanism for data transfers hold great promise as a new norm. While obligations captured in contractual clauses are dependent on signatories to ensure that the terms and conditions are implemented, certifications provide the assurance that an independent auditor has ensured compliance, and goes towards building a trusted network for cross border data flows.

6. Existing certification systems for cross-border transfers include the APEC Cross Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems. Recently, the Global CBPR Forum was launched to further facilitate multilateral cross border data flows. These are comprehensive certification mechanisms which ensure a consistent baseline level of data governance and protection across participating economies.

7. A further number of countries such as Japan and Singapore have domestic data protection certification systems. In Singapore, our domestic Data Protection Trustmark has been integrated with elements from the APEC CBPR and PRP Systems to simplify the application process. We are keen to work with other jurisdictions on mutually recognising existing domestic certification systems to promote cross border data flows.

Conclusion

8. With the shift towards a Digital Economy, it is imperative for economies to build common standards and principles together, to allow data to flow smoothly and safely across borders.

Me complace tener esta oportunidad de compartir la perspectiva de Singapur sobre los flujos de datos transfronterizos y la protección de datos personales. La capacidad de transferir datos personales a través de las fronteras es fundamental y esencial en una economía digital.

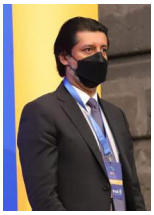
La ASEAN tiene un panorama diverso de protección de datos. El enfoque hacia la protección de datos y los desarrollos de privacidad varía de un país a otro, con países en diferentes etapas de madurez. A corto plazo, los contratos son un mecanismo básico eficaz para garantizar un nivel de protección comparable dentro de un área de diversidad, mientras que a largo plazo, el uso de certificaciones como mecanismo para la transferencia de datos es un camino muy prometedor.

Con el cambio hacia una Economía Digital, es imperativo que las economías juntas construyan estándares y principios comunes, para permitir que los datos fluyan sin problemas y de manera segura a través de las fronteras.

A cross-regional conversation: effective tools for secure-free data flows

Christopher Ballinas

General Director of Human Rights and Democracy
Minister of International Affairs, Mexico



These spaces for dialogue, such as those promoted by the Global Privacy Assembly, which allow the exchange of experiences, lessons learned, and best practices, are extremely valuable for raising protection standards and strengthening the capacities of state institutions in this area.

The issue on the right to privacy and personal data protection, particularly in the digital age, has been a priority of the Mexican foreign policy. That is why, within the framework of the Human Rights Council, Mexico is part of the group of countries that present the resolution on the right to privacy in the digital age, which includes rich content on the protection of personal data, and that has managed to be adopted by consensus.

The last resolution presented, adopted in 2021, focused on identifying the principal risks of artificial intelligence on the human right to privacy and other related rights, including the right to non-discrimination. In addition, the resolution called on States and companies to consider human rights obligations in the life cycle of new technologies.

In addition, to the international human rights instruments that refer to the right to privacy, Mexico is also part of the Convention for the protection of persons concerning the automated processing of personal data "Convention 108" and its Additional Protocol, which seeks to guarantee any natural person the respect of their right to private life concerning the automated processing of personal data, and that there is an authority responsible for assuring compliance with the Convention.

As you know, the Mexican State has also initiated the steps to sign the modernized Convention 108.

Technology and the digital age have allowed companies and different actors to collect data from users; therefore, there is still an enormous responsibility to regulate and ensure the personal data stored is protected.

Our identities are the most valuable thing we possess. Therefore, neutral and equitable algorithms must be generated with a human rights perspective, as it is one of the challenges we face today.

The digital age has allowed us to advance by leaps and bounds but also makes us vulnerable. Therefore, it is necessary to guarantee that there are mechanisms that will enable human intervention in decision-making that can be far-reaching and safeguard human rights in the digital age.

El tema del derecho a la privacidad y la protección de datos personales, en particular en la era digital, ha sido una prioridad de la política exterior mexicana. Es por ello, que en el marco del Consejo de Derechos Humanos, México formó parte del grupo de países que presentaron la resolución sobre el derecho a la privacidad en la era digital, la cual incluyó contenido sobre la protección de datos personales, y ha sido adoptada por consenso.

Además, México es Parte del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal "Convenio 108" y de su Protocolo Adicional. El Estado mexicano también ha iniciado las gestiones para suscribir el Convenio 108 modernizado (Convenio 108+).

Nuestras identidades son lo más valioso que poseemos, por ello, es fundamental que se generen algoritmos neutrales y equitativos con una perspectiva de derechos humanos, siendo este uno de los retos a los que nos enfrentamos hoy en día.

Andrea Jelinek

Chair of the European Data Protection Board

The Global Privacy Assembly is an important yearly appointment. Every autumn I look forward to our discussions and exchanges of best practices. For me, this panel touches upon the essence of the Global Privacy Assembly: learning from each other's experience and identifying where we can support each other and work together.

Since the outbreak of the COVID pandemic, ever more social and economic activities have moved online. With this, the importance of privacy and data protection is increasingly recognized.

In Europe, technological developments have driven the development of data protection laws since the 1970s, culminating in the adoption of data protection legislation in 1995. Twenty years later, the 1995 Data Protection Directive was due for a thorough make-over to answer the data protection needs of our time.

In Europe, we opted for one overarching law, to ensure a high level of legal certainty and transparency for both businesses and citizens. This drive for harmonisation led to the adoption of the General Data Protection Regulation or GDPR. It introduced "common rules of the game"; it creates a level playing field and ensures that data can move easily between

operators within Europe, while guaranteeing the consistent protection of individuals' personal data. We now have one set of privacy rules that are interpreted in a uniform manner throughout the European Economic Area (EEA), i.e. the European Union, Iceland, Liechtenstein and Norway.

As data move across borders, we also look beyond the geographical limits of the European Economic Area. The global dimension of our work is very important to us and we invest many resources in this.

In recent years, we've seen that the idea that individuals should have strong and enforceable data protection rights, guaranteed by an independent regulator, has been gaining ground worldwide. We also notice convergence around the idea that the protection of personal data must travel with the data when it is transferred. I find these developments very encouraging. They give me hope that, although differentiations and uncertainties remain, there is potential for worldwide convergence.

Naturally, we, at the EDPB, are available to exchange good practices with our colleagues worldwide. We are also eager to learn from other countries.

The Assembly shows that, despite the diversity of our legal cultures, backgrounds, instruments, we all share the same objective, the same driver, the same ideal:

protecting the rights of our people in the new digital era.

Through our joint efforts, I am sure that the convergence of our countries on data protection standards is just a matter of time.

En Europa, los avances tecnológicos han impulsado el desarrollo de leyes de protección de datos desde la década de 1970. Este impulso por la armonización condujo a la adopción del Reglamento General de Protección de Datos Europeo o GDPR, el cual introduce "reglas comunes del juego", crea condiciones equitativas, garantiza que los datos puedan moverse fácilmente entre operadores dentro de Europa, y salvaguarda la protección constante de los datos personales de las personas.

En los últimos años, hemos visto que la idea de que las personas deben tener derechos de protección de datos sólidos y exigibles, garantizados por un regulador independiente, ha ido ganando terreno en todo el mundo. Así como la idea de que la protección de datos personales debe viajar con los datos cuando se transfieren. Estos desarrollos me dan la esperanza de que, aunque persisten las diferenciaciones y las incertidumbres, existe potencial para la convergencia mundial.

Nosotros, en el EDPB, estamos disponibles para intercambiar buenas prácticas con nuestros colegas de todo el mundo y aprender de otros países.

José Luis Piñar Mañas, PhD

Professor of Administrative Law. Former Spanish Data Protection Commissioner. jlpinar@ceu.es

I thank INAI for the invitation to participate in such an important event and to do so in a panel on such an important topic and with such outstanding participants.

One of the most important challenges for data protection is to achieve a homogenous, and if possible binding, regulatory framework in a global world.

As is now commonly accepted, there are basically three models of data protection: the one based on the consideration of data protection as a fundamental right, the one that revolves more around consumer protection and the one that considers that personal data must be available to the public authorities. Most European and Latin American countries belong to the first model, as well as others we have in mind such as Australia, Canada or Japan.

I am convinced that the model that should prevail globally is the first one. This is, moreover, the model that most countries have implemented, even more so after the approval of the GDPR, which is undoubtedly the most important milestone that has ever taken place in favour of the globalisation of data protection, especially on the basis of its articles 3.2 (extraterritorial application) and 44 and following (international transfers).

But the effective guarantee of a right such as that of data protection, so conditioned by the massive, global and cross-border processing of personal information, is only possible if a high level of collaboration between States is achieved. This was from the outset the objective of the Ibero-American Data Protection Network, created in 2003, which in my opinion constitutes today the most relevant experience of transnational cooperation in the field of data protection, with the exception of the European Union, of course. The Declaration of La Antigua, Guatemala, signed on 6 June 2003, after affirming in point 2 "the consideration of the protection of personal data as an authentic fundamental right", states in point 5 that the signatories "note the need to promote the adoption of measures that guarantee a high level of data protection, as well as the suitability of having national regulatory frameworks which, inspired by common legal traditions, respect for fundamental rights and the interests of their respective countries, guarantee adequate protection in all the Ibero-American countries". This Declaration has favoured the approval of data protection laws in a large number of Ibero-American countries (there were only 3 or 4 laws when it was created), has inspired the creation of the "Association francophone des autorités de protection des données personnelles" and has promoted collaboration with the European Union.

But a further step towards a binding international legal framework is needed. Surely the United Nations should be much more active in the matter and promote an international text. But it should be ratified by the most relevant countries in data processing, something that would not pose problems, at least not in Europe or in most Latin American countries. But it would certainly pose problems in others.

The challenge is not easy. But it is necessary to achieve it. Because only from a global perspective can a fundamental right such as data protection, which operates on a global stage, be guaranteed.

Como es ya comúnmente aceptado, los modelos de protección de datos son fundamentalmente tres: el que se basa en la consideración de la protección de datos como un derecho fundamental, el que gira más en torno a la protección de los consumidores, y el que considera que los datos personales deben estar a disposición del poder público. Al primer modelo pertenecen gran parte de los países europeos y de América Latina, así como Australia, Canadá o Japón.

Estoy convencido de que el modelo que debe prevalecer a nivel mundial es el primero. Este es, además, el modelo que han implantado la mayoría de los países, más aún tras la aprobación del GDPR.

La efectiva garantía de un derecho como el de la protección de datos, tan condicionado por el tratamiento masivo, global y transfronterizo de información personal, sólo es posible si se alcanza un alto nivel de colaboración entre los Estados. El reto no es fácil. Pero es necesario conseguirlo. Porque solo desde una perspectiva global puede garantizarse un derecho fundamental como la protección de datos que opera en un escenario global.

Marguerite Ouedraogo Bonane

President of the Commission for Computing and Liberties (CIL) of Burkina Faso

From October 18th to 21st, 2021, the 43rd session of the Global Privacy Assembly (GPA) was organized in hybrid mode, given the international health situation linked to the COVID-19 pandemic, by the National Institute for Transparency and Access to Information and Protection of Personal Data (INAI) of Mexico. This annual event is an essential forum for personal data protection and privacy dialogue.

As a member of the Executive Committee of the GPA, I represented the African region, and we had the opportunity to speak on the topic: "Networks of Data Protection Authorities, from Regional Cooperation to Global Convergence". Cyberspace is a space in which citizens exchange at an instant speed that eliminates any notion of distance. In addition, the global and borderless nature of the Internet makes it difficult to regulate and enforce national laws within borders. It is necessary to adopt international legal norms.

In Africa, ECOWAS was the first regional organization to address the issue of personal data, adopting a harmonized legal framework to protect it. The African Union's initiatives reinforced these efforts by adopting the African Convention on Cyber Security and the Protection of Personal Data. These two texts constitute the legal and institutional framework for protecting personal data on the African continent.

These legal frameworks guarantee respect for the freedoms and fundamental rights of individuals, considering the prerogatives of the States, the rights of local communities, and the interests of companies.

In addition to these legal provisions, regional consultation frameworks are being created to promote the right to personal data protection. Among others:

• The Francophone Association of Personal Data Protection Authorities (AFAPDP) brings together the countries' data protection authorities and governments that share the French language. It offers support to States and authorities to develop local knowledge in the field of personal data protection based on the experience of the authorities that are part of the association.

• The RAPDP brings together the African authorities whose mission is to promote and supervise the protection of personal data in their countries, the States that plan to legislate on the protection of personal data, as well as the African associations and organizations that work in this area.

There is no doubt that personal data protection cannot be carried out in isolation and that cooperation between data protection authorities must be strengthened to be effective.

Therefore, we congratulate Mexico's INAI for its initiative and wish the GPA much success in its noble mission.

Long live the protection of personal data.

Thank you very much

En África, la CEDEAO fue la primera organización regional que abordó la problemática de los datos personales, adoptando un marco jurídico armonizado para protegerlos. Estos esfuerzos se vieron reforzados por la adopción de la Convención Africana sobre Ciberseguridad y Protección de Datos Personales, los cuales constituyen el marco jurídico e institucional de protección de datos personales en el continente africano.

Además se están creando marcos de consulta regionales encargados de promover el derecho a la protección de datos personales. Como la AFAPDP que reúne a las autoridades de protección de datos de los países que comparten el idioma francés, y la RAPDP**,** cuya misión principal es promover y supervisar la protección de los datos personales en sus países.

No cabe duda de que la protección de datos personales no puede llevarse a cabo de forma aislada y debe reforzarse la cooperación entre las autoridades para que sea eficaz.

Nelson Remolina Angarita

Associate Professor and Director of the Graduate School of the Law School of Universidad de Los Andes (Bogotá, Colombia). Former Deputy Superintendent for the Colombian Data Protection Authority. Former President of the Ibero-American Data Protection Network.

Data Protection Authorities and the Effective Protection of Human Rights on the Cyberspace.

Technological tools allow companies and organizations to collect data in any country without having a physical presence in the country's territory. These companies often argue that because they are not physically based in a country, the country's data protection law does not apply to them and their local authorities lack the competence to investigate them, give them instructions or sanction them.

Notwithstanding the foregoing, these organizations perform "technological presence" in the territories using the aforementioned tools or applications that are installed on equipment (phones, tablets, computers, etc.) located in the territory of any country.

To collect and process personal data in a country it is not necessary to be domiciled in the territory of that country. Internet and extraterritoriality cannot be synonymous with impunity or factors to disregard human rights, local regulations, and decisions of Data Protection Authorities.

What happens on the Internet in one part of the world can affect millions of people around the world. Therefore, it is necessary for authorities to strengthen their strategies to work as a team and react ex officio to cases of massive impact.

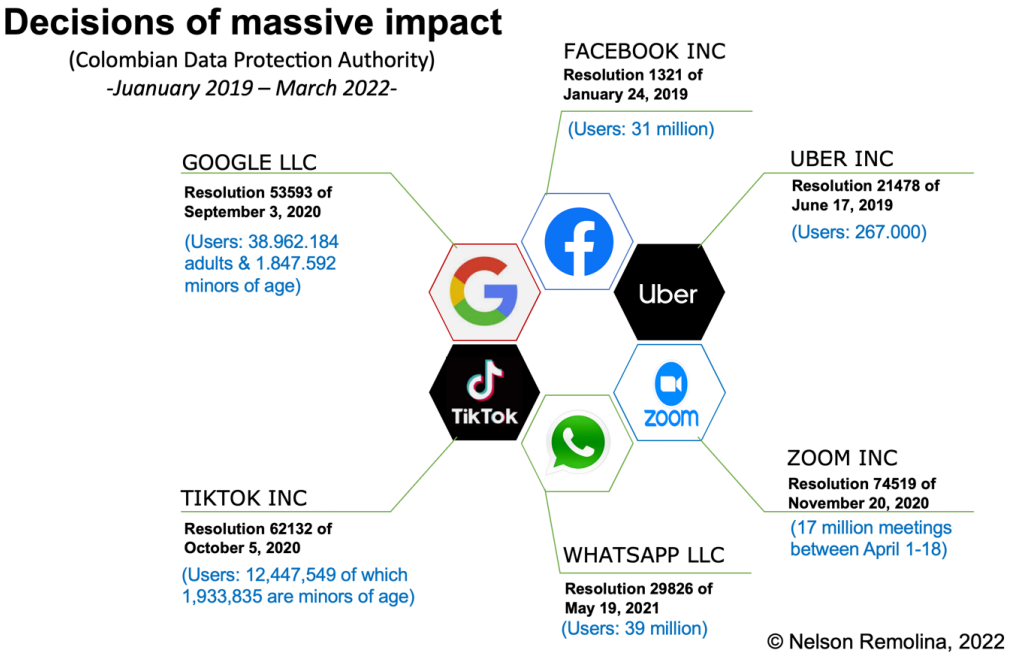
In this sense, the strategic plan of the Ibero-American Data Protection Network established the following strategy[7]: "4. **Towards the initiation of investigations into cases that impact data subjects in the countries of the network**. 4.1. Identify real cases that affect citizens of various countries of the network seeking that all the authorities of the network or most of them act ex officio and from their countries against such situations and within the framework of their legal competences".

Faced with this situation, Data Protection Authorities have initiated administrative proceedings against, among others, Google, WhatsApp, Uber, Facebook, TikTok and Zoom. Particularly, the Colombian authority (Office of the Deputy Superintendent for the Protection of Personal Data[8]) has deployed a series of actions to protect minors of age and adults whose data are collected and used by these organizations.

This chart summarizes the cases, highlighting the millions of people on whom these organizations hold data at the date of decision making:

[7] https://www.redipd.org/es

[8] https://www.sic.gov.co/tema/proteccion-de-datos-personales



Neither the Internet, nor the lack of territorial domicile or the lack of physical presence in a territory can be tools, phenomena, or arguments to promote or justify non-compliance with regulations regarding the processing of personal data and the violation of human rights.

Las aplicaciones tecnológicas instaladas en teléfonos celulares, tablets o computadoras, permiten recolectar datos personales a empresas y organizaciones de todo el mundo sin importar que se encuentren domiciliadas en un país determinado. Dichas empresas argumentan que no están sujetas a la ley de protección de datos personales de un país en el que no se encuentran físicamente. Pero internet no puede ser sinónimo de impunidad, infringir derechos humanos, ni leyes locales, y estar por encima de las decisiones que toman las Autoridades en materia de Datos Personales.

Es necesario, que dichas autoridades fortalezcan las estrategias que regulen los efectos del impacto masivo que las aplicaciones tecnológicas puedan causar. Ni el internet ni las empresas no domiciliadas pueden ser argumento para el incumplimiento de la normativa en materia de tratamiento de datos personales y la vulneración de los derechos humanos.

Consumer Rights, E-commerce, and Privacy Challenges

Josefina Román Vergara
INAI Commissioner, Mexico

In the face of the COVID-19 pandemic, the digitalization process of society was accelerated. Among the main factors that have become relevant is the electronic commerce, an activity of the digital economy from which personal data protection is linked to the free cross-border data flows.

In this regard, the issue of adequate data governance stands out, considering that in various regions, it has become an opportunity to strengthen relationships in the digital environment aiming to consolidate the mechanisms through which people interact, through different platforms of goods and services, and constitutes the main activity that generates value and promotes the rapid implementation of the digital economy.

It is important to seek a balance to provide trust and legal certainty to consumers since the lack of this trust in their privacy may be a factor that prevents them from obtaining the benefits of digital commerce. This brings us to the central theme of this session which is to reflect on important aspects as the principles and guarantees that must be implemented for data protection in electronic commerce, the convergence to guarantee the rights of consumers and their data, as well as the role that the authorities should play.

One of the central points to address the challenges of privacy in the electronic commerce depends on the approach from which the analysis is carried out, that is, if we see it from the point of view of the companies that offer goods and services in the digital market, specifically considering small and medium-sized companies, it will be important to think about issues related to the safeguarding of the rights of consumers as well as the due fulfillment of their obligations, specifically in privacy and personal data protection.

However, from the point of view of consumers, the interest relies in how to be able to access the digital market with the confidence that the personal information they provide will be protected; that is, that there is adequate management of their identity to mitigate risks of becoming victims of attacks by cybercriminals who seek to steal their identity. This is where issues arise regarding how to use digital identity mechanisms, that have the necessary

security measures to ensure the integrity, availability, and confidentiality of the information, can represent a competitive advantage in buying, selling, or exchanging goods, services and information through computer networks.

Likewise, it highlights the importance of protecting personal data and privacy, which are priority points when discussing the digital environment. This is because we can not carry out interactions without sharing personal data, which serves as the element that will allow us to recognize ourselves in cyberspace, and it's characterized by the enormous amount of personal data that is shared in it.

As more and more personal data is transferred and processed in the digital environment, there is an increasing need to create a secure environment by taking measures to protect society against deliberate misuse of data. Therefore, cybersecurity is extremely important from the personal data protection approach to managing and protecting the personal information shared by users in the digital environment.

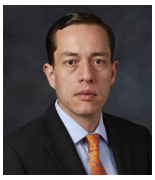
Ante la pandemia derivado del COVID-19, se aceleró el proceso de digitalización de la sociedad y entre los principales factores que han adquirido relevancia se encuentra el comercio electrónico. Al respecto, destaca el tema de la adecuada gobernanza de datos que constituye la actividad principal que genera valor y promueve la implantación rápida de la economía digital.

Es importante reflexionar en aspectos tan importantes como los principios y garantías que se deben implementarse para la protección de datos en el comercio electrónico, la convergencia para garantizar los derechos de las y los consumidores y sus datos personales, así como el papel que las autoridades competentes deben desempeñar.

A medida que se comparten y procesan cada vez más datos personales en el entorno digital, es cada vez más necesaria la creación de un entorno seguro a través de la adopción de medidas para proteger a la sociedad contra el uso indebido de los datos de forma deliberada.

Andrés Barreto

Commissioner at the Energy and Gas Commission of Colombia. Former Superintendent of Industry and Commerce of Colombia (SIC) (2018-2022)



The Superintendence of Industry and Commerce of Colombia is the Colombian Personal Data, Consumer and Competition Protection Authority. This privileged position has allowed the institution to deal with transversal issues in both, personal data and consumer protection something of great importance in the national and international sphere.

Consumers are also holders of personal data and maybe one of the challenges that we had faced is to harmonize the enforcement of both regimes. The idea is to adopt coordinated and efficient actions in order to protect consumer rights in e-commerce.

In our country, most of the complaints from consumers related to personal data referred to quality of information, failure to authorize data processing, unsolicited mass advertising (spam) and identity theft. The Deputy Superintendence for Data Protection has received in 10 years more than 90,000 complaints and in 2021 more than 2000. As a tool to respond to this type of phenomena, the SIC has created the SIC-FACILITA platform as an alternative mechanism to file consumer disputes. In addition, we had implemented several good practices like the Sandbox on Artificial Intelligence and privacy by design in e-commerce and marketing issues, aimed, among others, at entrepreneurs so that they are aware of the aspects of personal data protection.

This type of initiatives have also been shared in our participations as members of such a great and important international scenarios like the Organization for Economic Cooperation and Development (OECD), through the Consumer Policy Committee (CCP) and also through the Bureau of the Committee on Data Governance and Privacy in the Digital Economy (DGP) when I had the opportunity to act as a member of the Bureau.

La Superintendencia de Industria y Comercio de Colombia es la Autoridad de Protección de Datos Personales, Consumidores y Competencia de Colombia. Esta posición privilegiada le ha permitido a la institución tratar temas transversales tanto en materia de datos personales como de protección al consumidor.

En el país, la mayoría de las quejas de los consumidores están relacionadas con datos personales y refieren a la calidad de la información, la falta de autorización del tratamiento de datos, la publicidad masiva no solicitada (spam) y la usurpación de identidad.

Es por eso que entre las prácticas que hemos implementado tenemos la plataforma SIC-FACILITA como mecanismo alternativo para presentar disputas de consumo, un Sandbox sobre Inteligencia Artificial e iniciativas de privacidad por diseño relacionado a temas de comercio electrónico y marketing.

Isabel Davara F. de Marcos

Founding Partner-DAVARA ABOGADOS (Digital & Privacy Law Firm); Vicepresidenta INCAM; Consejera CGAM; Champion de Privacidad AmCham Mexico; Profesora ITAM; Abogada México y Madrid

In Mexico, consumers have diverse rights when acquiring products, goods or services offered by companies based in Mexico. Specifically, the Federal Consumer Protection Law lays down these rights and enshrines in its Articles 76 Bis and 76 Bis 1 those that suppliers or companies must guarantee in Internet transactions. Among these rights, of course, are the rights of privacy and personal data protection, which also entail the obligation to assure the security of the information processed through electronic means. However, it is important to consider that national laws have a particular application scope, and as a rule they are applicable to service providers established in Mexico.

In the assumption that Mexican laws are modified, and their scope of application is broadened, there is no doubt that the Industry and companies will have to comply with these provisions, therefore should be compliance and respect for the principles of legality and legal certainty stated by a Federal Law emanating from Congress, for example, companies not based in Mexico and complying with its provisions and consequently, guaranteeing the consumers rights. However, it is also true that, in practice, there are many national and international companies that already assume high compliance standards, even applying procedures and means like those established in other stricter jurisdictions. That is, it should not be forgotten that there are technology companies with high standards of compliance in regulatory and ethical aspects.

The industry desires to fulfill domestic law provisions that guarantee the rights of individuals and ensure possible investments and the future of the business. The law must therefore be the result of a broad deliberative process and a deep understanding of the industry and its nature.

In the region there is a significant disparity of standards and regulatory frameworks, and the authorities also have different capacities, strengths and weaknesses. Specifically, the region is experiencing a process of maturing, according to a global trend that follows the European model which is the most protective and advanced. Countries with recent data protection laws such as Brazil, Ecuador and Panama have laid down important rules for data processing based on the General Data Protection Regulation. In recent years we have seen that the legislations in the region have been maturing and this process seems to be as inexorable as the advance of technology itself.

However, in order to build a balanced and functional ecosystem in which innovation subsists and consumer rights are guaranteed, a trustworthy approach is required from the industry, where all stakeholders can feel comfortable sharing and learning. Industry must collaborate in a dynamic and free environment including the society and government to create a fairer and more balanced data protection ecosystem. The industry knows that data belongs to people and, of course, that it seeks to leverage it, but in a lawful manner at all times.

En México los consumidores tienen diversos derechos en el momento en que adquieren bienes, productos o servicios ofrecidos por empresas establecidas en México. Entre estos derechos, se encuentran los derechos de privacidad y protección de datos personales que también traen aparejada la obligación de garantizar la seguridad de la información procesada a través de medios electrónicos.

En la región existe una gran disparidad de normatividad y de enfoques regulatorios, además de que también las autoridades tienen diferentes capacidades, fortalezas y debilidades. La regulación en la región en específico está en un proceso de maduración.

A fin de construir un ecosistema equilibrado y funcional en el que la innovación subsista y se garanticen los derechos de los consumidores se requiere una aproximación confiable por parte de la industria, que todos los *stakeholders* puedan sentirse cómodos compartiendo y aprendiendo. La industria sabe que los datos conciernen a las personas y claro que deben buscar su aprovechamiento, pero siempre de una forma legítima.

Jennifer M. Urban

Chairperson of the Board C
alifornia Privacy Protection Agency, California, USA

Buenas tardes desde California, Los Estados Unidos, y muchas gracias por incluirme. I am honored to be here.

My name is Jennifer Urban. I am a Clinical Professor of Law at the University of California, Berkeley, in the United States. In March of 2021, I was appointed by California Governor Gavin Newsom to be the first Chairperson of the Board for the new California Privacy Protection Agency. Please note that my remarks are my own, and do not necessarily reflect the views of the California Privacy Protection Agency, its Board, or the State of California.

The California Privacy Protection Agency was created in November of 2020 via a ballot proposition —the California Privacy Rights Act ("CPRA")—, which amended the California Consumer Privacy Act of 2018 ("CCPA"). As a ballot proposition, the CPRA was directly approved by California voters. The Agency is tasked with implementing and enforcing these laws. California's Agency is a new endeavor —indeed, it is the first agency in the United States with full administrative powers focused on privacy and data protection— we thus hope to learn from authorities in other regions, which are rich with decades of experience. As Commissioner Denham noted during the Assembly, California's approach "stands firmly on the shoulders of existing" laws.

California's approach is informed by Europe's General Data Protection Regulation and other laws around the world. In the U.S., personal privacy and data protection law has long followed a distributed model. While there are federal laws that protect a few kinds of data —for example, medical data held by medical providers, student information, and credit data— the United States does not have a comprehensive federal data privacy law. Instead, privacy and data protection is distributed across sectors and states.

California's approach is also informed by its history as a leader in consumer privacy within the United States. California's state constitution explicitly protects the privacy of California residents, and California has led other U.S. states in developing consumer privacy protections. For example, among other things, California in 2003 enacted the first data breach notification law in the U.S. It is this tradition that the new law evokes when it charges the new Agency with "protecting the fundamental privacy rights of natural persons with respect to the use of their personal information" [California Civil Code, § 1798.199.40(c)].

Taken together, this background informs California's decision with the CCPA and CPRA to move away from old forms of the "notice and choice" model to a form that is easier for consumers to implement and provides an environment in which businesses can compete on privacy. By creating guardrails —for example, by prohibiting the use of "dark patterns;" and by requiring covered businesses to respond to universal "opt-out preference signals" that consumers can use to register their preferences across many businesses— the California law encourages privacy-protective business innovations and markets.

I look forward to further conversations, and to, as the California law charges the Agency to do: "Cooperat[ing] with other agencies with jurisdiction over privacy laws and with data processing authorities in California, other states, territories, and countries to ensure consistent application of privacy protections". [California Civil Code, § 1798.199.40(i)].

En los EE. UU., la ley de privacidad y protección de datos personales ha seguido durante mucho tiempo un modelo distribuido. Si bien existen leyes federales que protegen algunos tipos de datos, Estados Unidos no cuenta con una ley federal integral de privacidad de datos. En cambio, la privacidad y la protección de datos se distribuyen entre sectores y estados. El enfoque de California está basado en el Reglamento General de Protección de Datos de Europa, así como en otras leyes en todo el mundo.

La constitución del estado de California protege explícitamente la privacidad de los residentes de California, y ha servido como modelo para que otros estados de EE. UU. desarrollen sus protecciones de privacidad del consumidor, fomentando las innovaciones comerciales y los mercados.

La ley de California obliga a la Agencia a: "Cooperar con otras agencias con jurisdicción sobre las leyes de privacidad y con las autoridades de procesamiento de datos en California, otros estados, territorios y países para garantizar aplicación consistente de las protecciones de privacidad". [Código Civil de California, § 1798.199.40(i)].

Jules Polonetsky

CEO Future of Privacy Forum and former Consumer Affairs Commissioner, City of New York

Is data protection law the law of everything? Former Deputy Privacy Commissioner for New South Wales, Australia argues that "privacy law must become 'the law of everything', because in the digital economy, data about people *is* everything[9]. EU data protection law scholar Nadezhda Purtova declares that the broad definition of personal information in GDPR results in the law effectively becoming a "law of everything", a result she welcomes at present, but worries that it will be less practical as technology develops.[10]

But whether data protection is the law of everything or will one day be that expansive, it is clear that data protection law today already regulates a wide range of sectors dependent on data, from health, energy and transportation, to commerce, scientific research and social services. Few aspects of life today are not dependent on data, and thus subject to data protection law in many jurisdictions. Many of these sectors have been long regulated by statute, by common law, by ethical standards and industry norms, some for decades before data protection law came on the scene. Many of these sectors are subject to regulators or courts that increasingly provide guidance on the collection and processing of data, including personal data.

[9] https://www.salingerprivacy.com.au/2022/03/22/big-tech-blog/.
[10] https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176.

How is data protection law intersecting with these laws? In some cases, quite well, with new laws in industry sectors referencing the data protection statutes to ensure cohesive regulation. In some sectors, consumer, data protection, health, competition, transportation and other regulators are in close touch. But in many cases, data protection regulators see their role as independent and perhaps superior, as a reviewer of the conclusions of the decisions or these regulators, and this is indeed the case in some jurisdictions. In many areas, data protection law and other long established laws are developing without close coordination and in doing so creating conflict and confusion that courts will need to resolve.

One example of this dual track of legal development is the recent focus in data protection law on "dark patterns". Consumer protection law has long regulated the disclosures made when companies seek to induce a consumer transaction, whether personal data is involved or simply financial costs[11]. Is a dark pattern a handy term to reference already deceptive practices under consumer law, or does it set forward a more protective standard when personal data is involved? Rulemaking, DPA guidance and academic research is seeking to address this issue, but often without reference to current consumer protection requirements. Another example is the nature of a contract, when personal information is an issue, a topic where the relationship between contract law and the contractual basis for processing data under GDPR will be the subject of multiple court decisions.[12] Given space limitations here, I will mention one more case, that of the conflict between the reliance on "consent" by ethical review boards for sharing of clinical trial data for research purposes and the data protection guidance suggesting that patients cannot "consent" to such sharing as a legal basis.[13]

In each of these examples, and many more cases where data protection law is a "law of everything" in its scope, data protection experts will be most effective if we bring a sense of humility and of intellectual curiosity to understand the adjacent regulatory environments that we are expanding to cover. If we are so bold as to regulate a vast swath of the future of society, we need to be partners with those who are experts in the human rights that data protection law seeks to protect.

¿Es la ley de protección de datos la ley del todo? Está claro que la ley de protección de datos hoy en día ya regula una amplia gama de sectores que dependen de los datos, desde la salud, la energía y el transporte, hasta el comercio, la investigación científica y los servicios sociales. Muchos de estos sectores están sujetos a reguladores o tribunales que brindan cada vez más orientación sobre la recopilación y el procesamiento de datos, incluidos los datos personales.

En los casos en que la ley de protección de datos es una "ley de todo", los expertos en protección de datos serían más efectivos si aportamos un sentido de humildad y curio-

[11] file:///C:/Users/jules/Dropbox%20(Personal)/temp%20junk/FTC-2022-0035-0001_content.pdf.

[12] https://noyb.eu/sites/default/files/2021-07/Vorlage_sw_EN.pdf.

[13] https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en.

sidad intelectual para comprender los entornos regulatorios adyacentes que nos estamos expandiendo para cubrir. Si somos tan audaces como para regular una gran parte del futuro de la sociedad, debemos asociarnos con aquellos expertos en derechos humanos que la ley de protección de datos busca proteger.

Smart Cities and Mobility Hubs

Trevor Hughes

President and CEO of the International Association of Privacy Professionals (IAPP)

It is a pleasure to talk about smart cities and mobility hubs and the incredible number of issues they create in data protection and privacy worldwide.

In the past few years, we have seen the emergence of smart city implementations. There is massive complexity in the data environments associated with our cities and municipalities; it is not a single thing we are talking about. This is not a technology — it is many technologies. It is not a use of data — it is many uses of data.

The benefits of good implementations of smart cities can be enormous: improvements in social services; access to needed services; the efficiency of operations; greater engagement with citizens; greater delivery of services; and reductions in carbon emissions, among others.

The good use of data within these environments can be compelling but the risks can be challenging. The data collected can be susceptible, and the aggregation of this data in both public and private hands can be very tempting to look for secondary uses. There are specific uses of the data, sensor networks and other mechanisms for gathering data that we might see as challenging from a human rights perspective.

It's challenging to think of local governments as policy centers. Notably, local governments are notoriously under-resourced and unable to invest heavily in governance, compliance and program controls that might give oversight to smart city implementation. It must be clear that local governments must participate in discussing policy outcomes for smart cities. However, it is challenging to imagine a patchwork of various local governments all trying to address new policy standards for managing their implementation of a smart city. We find ourselves in the very early days of our consideration of data protection as one policy issue —a moment where if we interject with smart policy guidance—, we can make a difference where the role of well-informed and progressive data protection authorities can shape the future of these technologies.

To explore these challenges, let's consider these questions:

Why do we care?

• What are the key privacy/equity considerations as smart city/mobility hub efforts increasingly fuse the physical and digital realms?

• What regulatory initiatives have we seen to date? What has worked? What hasn't?

Where and how should this be regulated?

• What's the most appropriate level of government to regulate privacy for smart cities/mobility hub efforts (national, state, local, regional…)?

• Are local/regional bodies appropriately equipped to deal with sophisticated technology and privacy questions?

Is privacy even the right frame for policy issues in smart cities?

• What are the limits of privacy as a policy lens for managing the data governance challenges raised by smart cities? What other policy instruments and governance mechanisms do we need in tandem with privacy-focused remedies?

The role of the public

• When and how should smart city/mobility hub efforts engage the public/local communities in collective decision-making about appropriate uses of/protections for personal data?

• What role should public opinion play in designing data governance for smart cities?

The role of technology providers

• What is the role of technology providers/platforms in creating privacy solutions in smart cities?

All that data will be tempting

• How can smart city/mobility hub efforts make innovative uses of public data while still protecting the privacy of the individuals and communities represented in that data?

En los últimos años, hemos visto el surgimiento de implementaciones de ciudades inteligentes. Existe una enorme complejidad en los entornos de datos asociados con nuestras ciudades y municipios; no es una sola cosa de lo que estamos hablando. Esto no es una tecnología, son muchas tecnologías. No es un uso de los datos, son muchos usos de los datos.

El buen uso de los datos dentro de estos entornos puede ser convincente, pero los riesgos pueden ser un desafío. Los datos recopilados pueden ser susceptibles, y la agrupación de estos datos tanto en manos públicas como privadas puede ser muy tentador para buscar usos secundarios. Hay usos específicos de los datos, redes de sensores y otros mecanismos para recopilar datos que podríamos considerar desafiantes desde una perspectiva de derechos humanos.

Nos encontramos en los primeros pasos de nuestra consideración de la protección de datos como un tema de política, un momento en el que, si lo intercalamos con una guía política inteligente, podemos marcar la diferencia en el papel que las autoridades de protección de datos progresistas y bien informadas pueden dar forma al futuro de estas tecnologías.

Bruno Bioni

Director and co-founder of Data Privacy Brazil, founding partner of Bioni Consultoria.

The use of ICT as an urban management tool has come to leverage infrastructure efficiency for increasingly populated environments. "Smart cities", as they became known, describe the massive use of ICT as a possible solution for urban problems and, consequently, for improving the quality of life of citizens. Although the use of data collection and processing technologies is not new in the formulation of public policies, recent computational advances —Big Data, Internet of Things, artificial intelligence and the like— brought significant changes in quantitative and qualitative terms in data collection and processing. In this context, the transformation of the urban environment itself has made physical and informational infrastructure equally important for urban development —but more than that—, it has made clear the need for a holistic vision of an urban environment under reconfiguration with close attention to issues related to the protection of privacy and personal data of citizens.

In smart cities, the interdependence among physical and informational infrastructures unlocks new dimensions for (auto)monitoring and (auto)management of cities. This overlap occurs in an infosphere in which all the entities of an ecosystem —including citizens with their smartphones and sensors around them— are organisms that interact through the sharing of data. The operation of this environment is organized primarily through information flows that can influence or define a wide variety of aspects of the lives of citizens.

When we look at this phenomenon from an ecological perspective —that is, considering the relationships between beings (living and nonliving) and the environment, as well as their interconnection—, we are able to discuss not only the efficiency of public services and the solution of urban problems, but also everything in their midst for the purpose of sustainable development, which also includes protecting privacy and the capacity for self-determination of citizens.

In this sense, environmental factors must respect the existence of "privacy zones", into which individuals can withdraw (negative freedom) and control information (positive freedom) about themselves. For that, the legal architecture for exercising the right to privacy is as important as the technological architecture, and the interdependence between both structures —the "ecology of privacy"— must be driven into a sustainable direction. This means that the intensive use of ICT in urban environments should not reinforce the existing asymmetry in the relationship between citizens and the state, nor should it challenge the capacity of citizens to exercise self-determination in this ecosystem.

In the end, smart cities still raise challenges for policy making regarding whether massive processing of personal data through the use of ICT will in fact lead to better quality of urban life. For this to be a reality, urban policies should respect the historical development of the protection of personal data calibrated by transparency obligations. The protection of personal data is a condition for the capacity of self-determination by individuals and the collective body, and it is essential that the informational infrastructure of smart cities be subject to the public scrutiny of their inhabitants.

El uso de las Tecnologías de la Información y Comunicación en "las ciudades inteligentes" son consideradas como una posible solución para los problemas urbanos y de mejoramiento en la calidad de vida de los ciudadanos. Los avances computacionales recientes —Big Data, Inteligencia Artificial y similares— trajeron cambios en términos cuantitativos y cualitativos en la recolección y procesamiento de datos para las políticas públicas.

En las ciudades inteligentes, la interdependencia entre las infraestructuras físicas y de información abre nuevas dimensiones para el (auto)control y la (auto)gestión de dichas ciudades. El funcionamiento de este ecosistema se organiza principalmente a través de flujos de información que pueden influir o definir una amplia variedad de aspectos de la vida de los ciudadanos.

Dicho ecosistema de movilidad, debe respetar la existencia de "zonas de privacidad", en las que los individuos pueden controlar la información sobre sí mismos.

Kelsey Finch

Title: Senior Counsel, Future of Privacy Forum. @k_finch

As data protection and privacy have stepped into a spotlight on the global stage, there has been a flourishing of privacy activity at the local and community level that has been largely flying under the radar.

Cities and local governments around the world are embracing a multitude of connected or "smart" technologies and mobility services in order to make their communities more livable, equitable, and sustainable. During the early wave of the COVID-19 pandemic, for example, cities studied traffic and mobility patterns, public health data, and connected sensors to make decisions about closing roadways to enable open-air restaurants and social distancing.

At the same time, these technologies raise concerns about individual privacy, freedom of choice, and institutional discrimination. Local governments have been tasked with answering the important question: How do we leverage the benefits of a data-rich society while giving members of our community the confidence of knowing their privacy is protected? How can we address pressing local problems —from housing to highways, potholes to policing— and deliver public services in equitable, privacy-conscious ways?

Smart city initiatives bring the privacy risks of new technologies closer to home; they can spur privacy innovation close to home as well. In countries without national regulations, many "smart cities" and communities have proactively established their own privacy and data protection programs, including: establishing city-wide privacy principles reflecting local values; passing local ordinances to control the acquisition and use of surveillance technologies; restricting facial recognition technologies or other sensitive data collection in public spaces; hiring Chief Privacy Officers and dedicated privacy experts; conducting and publishing privacy or data protection impact assessments; setting procurement standards to require privacy by design and default; establishing community oversight and advisory bodies; and more.

Critically, while many local governments are establishing more transparent, accountable internal data practices, they are also increasingly providing members of the public opportunities to

meaningfully participate in decision-making about how personal data is processed within their communities. "Smart city" technologies raise unique challenges because they operate in shared, public spaces. Conversations about personal data, in these contexts, are most often also conversations about ethics, equity, and how to make collective decisions when the risks and benefits to individuals can vary wildly, even within communities.

Smart city initiatives shine a light on the impacts of emerging technologies and data flows, and local governments have unique opportunities to foster important discussions about privacy, trust, power, and fairness. Unfortunately, local governments often lack the dedicated resources and expertise to advance these efforts on their own. I encourage everyone who took part in this Global Privacy Assembly to seek out opportunities to contribute your experience and expertise within your own local community as well.

Las ciudades y los gobiernos locales de todo el mundo están adoptando una multitud de tecnologías y servicios de movilidad conectados o "inteligentes" para hacer que sus comunidades sean más habitables, equitativas y sostenibles. Al mismo tiempo, estas tecnologías plantean preocupaciones sobre la privacidad individual, la libertad de elección y la discriminación institucional.

En países sin regulaciones nacionales, muchas "ciudades inteligentes" y comunidades han establecido proactivamente sus propios programas de privacidad y protección de datos, que incluyen: establecer principios de privacidad en toda la ciudad que reflejen los valores locales; aprobar ordenanzas locales para controlar la adquisición y el uso de tecnologías de vigilancia; restringir las tecnologías de reconocimiento facial u otra recopilación de datos confidenciales en espacios públicos; y más.

Las tecnologías de "ciudades inteligentes" plantean desafíos únicos porque operan en espacios públicos compartidos. Sin embargo, arrojan luz sobre los impactos de las tecnologías emergentes y los flujos de datos, y los gobiernos locales tienen oportunidades únicas para fomentar debates importantes sobre la privacidad, la confianza, el poder y la equidad.

Suzanne Hoadley

Senior Manager- Coordinator Traffic Efficiency at Polis

Two pivotal moments have greatly influenced local authority attitudes towards transport data and how they work with it. The first was the open data movement, which kicked off around 2010 in Europe. Prior to open data, transport data was largely considered a by-product of (transport management) systems and consequently held little value. Open data revealed the value of data and the need for it to be properly managed to harness its full potential. The second pivotal moment was the adoption of the EU's landmark data privacy legislation, the General Data Protection Regulation (GDPR), in 2016. The regulation has forced every organisation, public or private, to carry out a comprehensive review of its interaction with data and to introduce procedures to ensure data policy and practices are in line with the provisions and principles of GDPR.

Local authorities today are gradually building up their data capability, particularly developing data skills, investing in data projects (such as data lakes), analysing data sets (to gain insights) and generally reviewing their data needs and how to source the data. This is an ongoing process and it is happening in a context of constant change regarding technology (generating more and more data) and market dynamics (growth in the number of data players and new business models). GDPR is a common backdrop to all these developments and is influencing most data activities to a greater or lesser degree.

Data privacy is a dominant theme in two recent data developments involving local authorities. The first concerns data shared by operators of shared mobility services, particularly eScooters and bikes. To get a grip on the rapid growth of these free-floating services that have taken over our streets, cities are demanding data about their operation for monitoring, enforcement and mobility planning purposes. The second area relates to the growing interest among local authorities in gathering data about the flow of active modes (walking and cycling) with the aim of understanding the impact of policies and of informing transport planning.

In both cases, although the data shared or gathered contains no personal details (such as a name or address), it is nonetheless perceived as personally identifiable since it may be linked to an individual trip. This is giving rise to debates about data privacy and has been a cause for concern around the world, not least in the US where there has been some resistance from service providers to share data with governments but also in the EU, including the example of a Dutch court fining a municipality for monitoring people movements through the free public WiFi (https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-municipality-wi-fi-tracking_en).

The uncertainty and perceived conflicts with data privacy legislation is leading city authorities to err on the side of caution in acquiring data from external sources. Many are choosing to acquire highly aggregated data, yet GDPR does not prohibit the sharing and processing of personal data provided there is a valid reason to do so. This situation demonstrates that there is a need for an analysis of the application of the horizontal piece of legislation that is GDPR to the vertical and data-rich sector of mobility.

Dos momentos cruciales han influido en las autoridades locales hacia los datos de transporte y cómo trabajan con ellos. El primero fue el movimiento de datos abiertos, que comenzó alrededor de 2010 en Europa. Antes de los datos abiertos, los datos de transporte tenían poco valor. Los datos abiertos revelaron el valor de los datos y la necesidad de gestionarlos adecuadamente para aprovechar todo su potencial. El segundo momento fue la adopción de la legislación de privacidad de datos histórica de la UE, el Reglamento General de Protección de Datos (GDPR), en 2016.

La privacidad de los datos es un tema dominante en dos desarrollos de datos recientes que involucran a las autoridades locales. El primero se refiere a los datos compartidos por los operadores de servicios de movilidad compartida. El segundo se relaciona con el creciente interés de las autoridades locales por recopilar datos sobre el flujo de modos activos (caminar y andar en bicicleta) con el objetivo de comprender el impacto de las políticas y de informar la planificación del transporte.

Issues concerning the processing of personal data in the electoral arena

Colin J. Bennett

Professor Department of Political Science
University of Victoria, BC. Canada

At the center of efforts to combat electoral manipulation and propaganda stands the question of how personal data on individual voters is being processed and whether or not it is done so legally and ethically. Familiar data protection questions are now injected into this heated international debate about democratic practices, and international DPAs now find themselves at the center of a global conversation about the future of democracy.

There is a rich tradition of understanding the role of effective privacy protection within different forms of democracy. For liberal democracy, privacy advances individual autonomy and self-fulfillment and reinforces political competition. For participatory democracy, privacy bolsters participation and engagement: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism, and protesting. For deliberative democracy, privacy enhances the freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values, and interests of others.

We know that privacy is essential for democracy. Until recently, we have known relatively little about how privacy has been compromised by democracy and by the agents that seek to mobilize, engage and encourage us to vote – or not to vote.

Modern political campaigns worldwide are now meant to be "data-driven" to consolidate existing support and find potential new voters and donors. Some campaigns construct detailed profiles on individual voters to "micro-target". The balance between privacy rights, and the rights of political actors to communicate with the voters, will be struck in different ways in different jurisdictions depending on a complex interplay of legal, political, and cultural factors.

The overall balance will also be affected by the party system, the electoral system, and campaign financing rules. The balance will also be influenced by the political culture and, in particular, the general acceptability of direct candidate-to-voter campaigning practices,

such as door-to-door canvassing or telephone polling. In countries with recent memories of authoritarian rule, data on political affiliation sensitivity is particularly acute. In some countries, it is not customary for voters to display symbols of political affiliation on their persons, cars, or houses–as in others.

It is widely argued that elections must now be data-driven to be effective. Still, there is nothing inevitable about these trends. The larger question is how much information political parties and candidates should have about those citizens to perform their essential roles? In general terms, how much should the political speaker be allowed to know about the audience to speak effectively?

Entre los esfuerzos para combatir la manipulación electoral y la propaganda se encuentra la cuestión de cómo se procesan los datos personales de votantes individuales y si se hace de manera legal y ética.

Sabemos que la privacidad es esencial para la democracia. Hasta hace no mucho tiempo sabíamos relativamente poco acerca de cómo la privacidad ha sido comprometida por la democracia y por los agentes que buscan movilizarnos, involucrarnos y animarnos a votar o no votar. Las campañas políticas modernas en todo el mundo ahora están "basadas en datos" para consolidar el apoyo existente y encontrar nuevos votantes y donantes potenciales.

Se argumenta ampliamente que las elecciones ahora deben estar basadas en datos para ser efectivas, y para ello las campañas construyen perfiles detallados de votantes individuales como "microobjetivos". El equilibrio entre los derechos de privacidad y los derechos de los actores políticos a comunicarse con los votantes se logrará de diferentes maneras en diferentes jurisdicciones dependiendo de una compleja interacción de factores legales, políticos y culturales.

James Dipple-Johnstone

Deputy Commissioner and Chief Regulatory Officer. ICO, UK

• When we launched our investigation in 2017, we were aware of the potential seriousness of the issues.

• However, we did not expect it would expand to be the largest, most complex and longest running carried out by our authority. Indeed, some work is only now coming to a close.

• The investigation has received much coverage, but this work includes a series of audits of 11 major political parties in the UK, leading to **497** recommendations about their compliance with the UKGDPR; these have since been followed up.

• Our investigation discovered a wider ecosystem of large, well-established trading and profiling of personal data.

• There is a sometimes brittle relationship between privacy and democratic institutions. As a result of our work we concluded that there are vulnerabilities in our democratic systems.

• We have previously spoken at the GPA in some detail about our findings. The lessons from what we learnt from such a wide-ranging and in some ways pioneering investigation for our office, and what progress has been made since, are:

1) Lesson 1: Technological developments have changed the rules of the game.

2) Lesson 2: A modern approach to regulation is essential.

3) Lesson 3: data protection regulation is cross-cutting.

4) Lesson 4: Effective regulation requires coalitions.

• Progress has been made in this area. The action we've taken has had a significant impact on the political campaigning ecosystem. It brought about increased transparency and better practices contributing to the upholding of electoral integrity.

• And we have set out our expectations for the future by publishing the ICO's political campaigns guidance that provides a framework for the use of personal data in the age of digital elections.

• Transparency around online political advertising and messaging is key. Voters should know who is responsible for the messages they receive and why they are receiving them. This matches the feedback we've seen from voters themselves.

• Some social media platforms stopped direct political party or campaigning adverts while others have made some efforts to improve transparency around political ads.

• We know that many political parties have acted on our audit recommendations and made significant improvements to their accountability arrangements.

• The UK Parliament intends to consider a new Elections Bill taking forward improvements to the election process in the UK, including mandating digital imprints.

• The Government's recent consultation on data protection reform also includes a number of questions around the interface between UK data protection regime and democratic engagement.

• But we know there is more to be done. We have seen some terrible examples of how the messaging itself needs attention in the on-line harms context.

• This is not an easy or quick issue to fix but instead goes to the heart of how society will engage with the democratic process in the future.

• We recognise that political parties need to be able to communicate effectively, using the range of modern communications methods available. However, it is also vital this communication is done in ways that foster public trust in how our data is being used.

En el 2017 lanzamos una investigación sobre el tema de elecciones digitales en la que se descubrió que existe una relación frágil entre la privacidad y las instituciones

democráticas. Como resultado de nuestro trabajo concluimos que existen vulnerabilidades en nuestros sistemas democráticos.

Las lecciones de lo que aprendimos son:

1) Lección 1: Los avances tecnológicos han cambiado las reglas del juego

2) Lección 2: Un enfoque moderno de la regulación es esencial

3) Lección 3: la regulación de protección de datos es transversal

4) Lección 4: La regulación efectiva requiere coaliciones

Por ello, realizamos una publicación de la guía de campañas políticas del ICO que proporciona un marco para el uso de datos personales en la era de las elecciones digitales.

Reconocemos que los partidos políticos deben poder comunicarse de manera efectiva, utilizando la variedad de métodos de comunicación modernos disponibles. Sin embargo, también es vital que esta comunicación se realice de manera que fomente la confianza pública en cómo se utilizan nuestros datos.

Michael McEvoy

Information and Privacy Commissioner for British Columbia, Canada. @BCInfoPrivacy

Among Canada's privacy regulators, British Columbia is unique in having authority to oversee the activities of political parties. Canada is a federation where the federal and provincial government's have jurisdiction over data protection. The provincial authorities can legislate in the privacy realm so long as their legislation is substantially similar to that of the federal government.

The British Columbia *Personal Information Protection Act* (PIPA) applies to any organization located within BC that collects, uses, or discloses personal information of any individuals inside or outside of BC.

My own history with political parties stems from work I undertook with the UK Information Commissioner's Office on the Facebook/Cambridge Analytica scandal. On returning to British Columbia as Commissioner my Office joined with the Federal Office of the Privacy Commissioner (OPC) to examine the Facebook/Cambridge Analytica matter as it affected Canadians. We again combined resources with the OPC in issuing an investigation report in November 2019 into AggregateIQ data services, a Victoria-based company that worked with Cambridge Analytica and organizations supporting the leave forces in the referendum on the European Union.

As significantly, my Office used its authority over political parties to issue an investigation report entitled Full Disclosure: Political parties, campaign data and voter consent released in February 2019, which among other things held that inferred data and support scores are the personal information of voters and must be disclosed to them if requested.

In addition, based on complaints we received, we have issued two orders in which it was determined that federal political parties operating in BC came within my jurisdiction. In one of those cases, I found the party in question collected information in contravention of our Act.

In a similar vein, we are presently adjudicating a complaint regarding the use of information by all major federal political parties and about which I am unable to comment because it is an ongoing matter. We are also actively investigating one federal political party's use of facial recognition technology for verifying individual's identification in virtual nomination races. Finally, we have successfully partnered with our elections regulator to develop a code of practice, agreed upon by all major political parties, that jointly deals with privacy and campaign-related obligations.

How have campaign technologies pioneered in the US influenced campaigning in your jurisdiction?

Data technologies developed in the US have undoubtedly influenced Canadian political campaigns and we are certainly seeing more data driven campaigns here in our country.

What are the major data protection questions raised by modern digital campaigning, and the use of social networking tools in political campaigns?

Vast amounts of personal information that in itself may have been necessary for analog campaigns (like voter lists) are supercharged today by data linking and advanced modelling techniques. Use of this data for techniques to manipulate voter behaviour assault the integrity of citizens and the democratic process itself. The recent Facebook revelations reveal how that platform's algorithm allows for political parties to both engender extreme political campaigning as well as suppress voter participation.

What are some of the key challenges for DPAs in the investigation of political organizations, as opposed to commercial of governmental organizations?

Political parties see themselves as "special" and often beyond the scope of regulation because of the space they occupy in the democratic process**.** Those that end up in power also ultimately decide how legislation will affect their own activities. In Canada, there has been a reluctance thus far to meaningfully regulate these activities by the current government. The highly competitive nature of political campaigns also means parties are extremely reluctant to engage in constructive enforcement or soft regulation.

How should a DPA go about conducting investigations of political parties and campaigns?

DPAs should, in my opinion, use the same process as any other investigation.

What are some of the regulatory tools that DPAs should consider applying to the political campaigning arena —for example, do codes of practice play a useful role—?

Codes of practice likely do play a role. We are trying that method here but as with any voluntary tool the difficulty is in the enforcement of a code versus legislation**.** Public pressure or negative media attention can also be very useful.

What is the appropriate relationship between the DPA and the election regulatory agency?

Increasingly, we are finding collaboration between different regulators to be helpful and essential to some of these cross-sectoral issues. In the case of political parties, we are working with the Chief Electoral Officer of BC on a Code of Practice.

Entre las autoridades reguladoras de privacidad de Canadá, la de Columbia Británica es la única que tiene facultad para supervisar las actividades de los partidos políticos. Mi propia historia con los partidos políticos proviene del trabajo que realicé en la Oficina del Comisionado de Información del Reino Unido en relación al escándalo de Facebook/ Cambridge Analytica.

De manera significativa, mi Oficina usó su autoridad sobre los partidos políticos para emitir un informe de investigación titulado Divulgación completa: Partidos políticos, datos de campaña y consentimiento de los votantes publicado en febrero de 2019, que, entre otras cosas, sostenía que los datos inferidos y los puntajes de apoyo son información personal de los votantes y solo debe ser revelado si ellos así lo solicitan.

Así mismo, de la mano de nuestro regulador electoral hemos desarrollado un código de práctica, acordado por todos los principales partidos políticos, que aborda de manera conjunta la privacidad y las obligaciones relacionadas con las campañas.

Tobias Judin

Head of International at the Norwegian Data Protection Authority

The juxtaposition of fair elections and the adtech industry

At the Norwegian Data Protection Authority, we were disappointed to find that the largest Norwegian political party broke the law when it in 2013 extracted party members' friend lists from Facebook. The lists were combined with data from other sources, and the purpose of this exercise was to ascertain whether the listed individuals were 'likely sympathisers' that could be persuaded to vote for the party.

In our view, this amounted to political profiling, and for most of people, their political views are sensitive and private. The case also raised an issue of transparency, as the likely or unlikely sympathisers were not given information about the processing of their data. Our concern is that information asymmetry may be leveraged to unduly affect the decisions —or votes— of individuals.

In 2019, we launched a fact-finding mission to learn more about the data processing practices of the established political parties in Norway. While we were happy to learn that our political parties avoid microtargeting, we found the general level of data protection maturity amongst them rather underwhelming. Furthermore, the general assumption appeared to be that if a tracking or marketing service is offered by an established platform, it must automatically be lawful for political parties to use also in an electoral context. This assump-

tion runs contrary to the principle of accountability, and it could lead to unlawful processing of voters' personal data.

Nevertheless, one thing became clear to us: Our political parties do not have ill will. They do not want to violate data protection rules in any way. There is no evidence that their processing of personal data has actually prejudiced democratic elections.

Unfortunately, political parties are not the only data controllers that we need to worry about. Other entities may also have an interest in affecting voters or the integrity of our elections. Rouge players may go further than the established political parties in terms of political profiling, microtargeting, or even targeted disinformation. A key issue is whether we have the capabilities to discover such actions and the resilience to safeguard our elections against them.

Which political messages will *you* see on social media? Equally interesting is perhaps the question of who is excluded from receiving the same information, and why. The personal data driven personalisation algorithms of private companies are exercising an ever-increasing influence on the freedom of information.

As long as opaque and invasive advertising options are available, we cannot expect that those options will never be utilised to interfere with our elections. Therefore, we need to turn our attention towards the systemic issues of the adtech industry more generally. While we cannot avoid that hostile entities will try to manipulate voters, we can regulate the practices and capabilities of the platforms they use to reach them, and thus minimise the potential for harm accordingly.

En la Autoridad de Protección de Datos de Noruega, en 2019, realizamos una investigación para obtener más información sobre las prácticas de procesamiento de datos de los partidos políticos noruegos. Si bien nos alegró saber que nuestros partidos políticos evitan la microfocalización, encontramos que el nivel general de madurez de la protección de datos es bastante decepcionante.

Una cosa nos quedó clara: Nuestros partidos políticos no tienen mala voluntad. No quieren violar las normas de protección de datos de ninguna manera. No hay evidencia de que su procesamiento de datos personales haya perjudicado realmente las elecciones democráticas.

Si bien no podemos evitar que entidades hostiles intenten manipular a los votantes, podemos regular las prácticas y capacidades de las plataformas que utilizan para llegar a ellos y, por lo tanto, minimizar el potencial de daño en consecuencia.

Digital Identity: Digital Rights and Privacy impacts in a hyper-connected society

Estelle Masse

Europe Legislative Manager and Global Data Protection Lead at Access Now

Governments around the world have been developing digital identity programmes. While there is a general assumption that these programmes can streamline administrative processes and empower users, they can in fact lead to significant privacy and data risks.

In some countries, it is mandatory for people to be enrolled in digital identity programmes in order to access essential services such as health benefits, social care and services, education programmes, or voting systems. This leads to exclusionary outcomes. Vulnerable groups unable to enroll, due to a variety of circumstances, such as poor technology infrastructure or gaps in technology design, are not able to exercise basic rights. A digital identity should not be a precondition to access basic services and rights.

The design of digital identity systems may lead to significant privacy and security risks. For instance, a centralised digital identity framework can lead to tracking everyday activities of a user. It can also end up creating a single point of failure in case of unauthorised access as it gathers sensitive information of communities and even entire populations. With centralised architectures, one breach into the ecosystem could jeopardise the safety of the database and the security and integrity of the data held. Centralised models, which are currently the most common models used for digital identity, represent a high-risk for data security.

Centralised models create the risk of 360 degree profiling and surveillance of users by governments and private actors with access to the databases associated with such programmes. Such an ecosystem can be hugely detrimental to the fundamental rights to privacy and data protections of users. The problem is accentuated in countries which lack comprehensive privacy and data protection frameworks, have compromised institutional standards, and have weak independent oversight and enforcement standards. In such countries, financial incentives and industry needs often overtake human rights considerations. As a result, privacy and data protection protections are delayed or weakened.

Challenges also exist in countries where data protection laws are in place. Data protection regulators may have limited power to launch investigations or to oversee the human rights impacts of digital identity systems in a comprehensive manner, including impacts on the right to non-discrimination.

Beyond digital rights, addressing the impact of digital identity programmes requires assessing populations' needs. All too often, systems are designed and implemented without a recognition of regional and local realities and without the consultation of key stakeholders including the most vulnerable.

En algunos países, es obligatorio que las personas se inscriban en programas de identidad digital para poder acceder a servicios esenciales como beneficios de salud, atención y servicios sociales, programas educativos o sistemas de votación. Si bien existe la suposición general de que estos programas pueden optimizar los procesos administrativos y empoderar a los usuarios, también pueden generar riesgos significativos para la privacidad y los datos conduciendo a resultados excluyentes.

Los grupos vulnerables que no pueden inscribirse debido a una variedad de circunstancias, como una infraestructura tecnológica deficiente o brechas en el diseño de la tecnología, no pueden ejercer los derechos básicos. Una identidad digital no debe ser una condición previa para acceder a servicios y derechos básicos.

Más allá de los derechos digitales, abordar el impacto de los programas de identidad digital requiere evaluar las necesidades de las poblaciones. Con frecuencia, los sistemas se diseñan e implementan sin reconocer las realidades regionales y locales y sin consultar a las partes interesadas, incluidos los más vulnerables.

Anita L. Allen, JD., PhD

Henry R Silverman Professor of Law and Professor of Philosophy. University of Pennsylvania Carey School of Law. Affiliated Faculty, Center for Technology, Innovation and Competition. Affiliated Faculty, Department of Africana Studies. Affiliate Faculty, Warren Center for Network & Data Sciences. Senior Fellow, Leonard Davis Institute for Health Economics

National Identification Cards and Personal Identity

The United States does not have a national identification card. Americans rely upon state-issued identification cards, drivers' licenses, Social Security numbers, passports and even credit cards to help establish their identities for purposes of gaining access to goods and services, including air travel.

In 2023 Americans will be required to show what is being called a REAL ID to travel on commercial aircraft facilities. A real idea will be a form of identification that meets minimum security standards established by the federal government. The impetus behind the REAL ID has been national security.

The tragedy of September 11, 2001 in which terrorists commandeered four aircraft targeting, inter alia, the World Trade Center in New York City and the Pentagon in Washington D.C. was made easier by a lack of a secure national identification standard. As explained by the Department of Homeland Security: "The REAL ID Act, passed by Congress in 2005, enacted the 9/11 Commission's recommendation that the Federal Government "set standards for the issuance of sources of identification, such as driver's licenses. The Act established minimum security standards for license issuance and production and prohibits certain federal agencies from accepting for certain purposes driver's licenses and identification cards from states not meeting the Act's minimum standards". Privacy advocates were skeptical of the REAL ID scheme, and there has long been a philosophical objection in the United States to a general-purpose national identification system that would disable to ability to move about anonymously.

It seems inevitable now that Americans will have digital identities both imposed by law and created by the electronic tracking, tracing, and monitoring of their activities in a digital economy. As the experiences of American black and brown men and women attest, the United States is already a surveillance society watchful and discriminatory, even without a national ID card or the REAL ID.

By contrast to the United States, the National of India has adopted a truer national identification card — the Aadhaar card. Aadhaar is described as "a strategic policy tool for social and financial inclusion, public sector delivery reforms, managing fiscal budgets, increase convenience and promote hassle-free people-centric governance". To access government services, the 1.3 billion people of India are expected to have a unique 12 digit identifier issued by the government based on an iris scan, a fingerprint and demographic information. In the Indian Supreme Court case of *Putttswamy v. Union of India* in 2018, the high court held that constitutional "right to privacy" would potentially limit the Aadhaar mandate if it did not meet standards of data protection. The Aadhaar program moved forward. The government has assured that the "Aadhaar number is devoid of any intelligence and does not profile people based on caste, religion, income, health and geography". It must be hoped that privacy as well as nondiscrimination can be truly guaranteed into India's future.

Estados Unidos no cuenta con una tarjeta única de identificación nacional. Los estadounidenses confían en las tarjetas de identificación emitidas por el estado, licencias de conducir, números de Seguro Social, pasaportes e incluso tarjetas de crédito para establecer sus identidades con el fin de obtener acceso a bienes y servicios, incluidos los viajes aéreos.

En 2023, los estadounidenses deberán mostrar lo que se denomina REAL ID para viajar en instalaciones de aviones comerciales bajo el cumplimiento de estándares mínimos de seguridad establecidos por el gobierno federal. Ahora parece inevitable que los estadounidenses tengan identidades digitales tanto impuestas por la ley como creadas por el seguimiento, rastreo y monitoreo electrónico de sus actividades en una economía digital.

A diferencia de los Estados Unidos, la India ha adoptado una tarjeta de identificación nacional más verdadera: la tarjeta Aadhaar. Aadhaar se describe como "una herramienta

de política estratégica para la inclusión social y financiera, las reformas del sector público, la gestión de los presupuestos fiscales, el aumento de la comodidad y la promoción de una gobernanza centrada en las personas sin complicaciones".

Leonardo Cervera Navas

Director at European Data Protection Supervisor.
LinkedIn: Leonardo Cervera Navas.
@cerveranavas

Q. What is the relationship between digital identity and the latest technological innovation tools that use artificial intelligence?

Depending on the intention, AI technologies can be used both to the benefit and to the detriment of individuals' rights. For example, biometric authentication technologies allow verification of individuals' identities and subsequent allocation of rights to them, whereas the use of deepfakes is linked to fraud and identity theft incidents.

The application of AI technologies for authentication requires a careful assessment of their capacities, limitations and risks stemming from their characteristics (e.g. complexity, opacity and dependence on data, bias). Any digital identity management system using AI needs to consider the probabilistic nature of many of them and put in place appropriate risk mitigation measures. The requirement of data protection by design needs to be complied with.

When AI is used in the context of identity authentication, the relevance of transparency cannot be underestimated. Transparency is needed so that individuals know, among others, that their personal data are processed with AI, understand the purposes for such processing and be informed whether AI is used to take any automated decisions. In case of the latter, the digital identity management system would require effective human oversight to comply with Article 22 of the GDPR.

Q. Is digital ID necessary in a hyper-connected society? Are we responding to an industry need or a user/public need?

Having one or more digital identities is a necessity that has been acknowledged a long time ago. The EU has been legislating on this topic for over two decades. The European Commission's proposal for a European Digital Identity regulation, amending the eIDAS Regulation, is just the last step. My home country, Spain, was a pioneer in digital identity and started the provision of electronic ID cards to all citizens in 2006.

The pandemic increased the pace at which EU citizens moved their daily activities from the analogical to the digital sphere. Consequently, the need for a well-designed and secure digital ID has become increasingly urgent.

Digital identities will always be necessary for some online activities such as banking, shopping or allowing citizens to communicate with public authorities (e.g. lodge complaints or pay taxes). In that respect, a digital identity serves the needs of public authorities, of users and of private sector.

The question is not so much if digital identities are necessary, but if they should be mandatory in all contexts and who should be in control of them. Some perceive digital identity frameworks as the first brick of a massive surveillance system. It does not have to be that way and we need to make it sure it will not be that way.

The Internet will always need space for anonymity and privacy and digital identities should be used only when necessary and not by default. We need to protect people's privacy by allowing them to use digital identities when they need to but also allowing them not to use them when it is not necessary.

In any case, we all have multiple identities in the real life [in my case: EU official, husband, father, home owner, author,-...], so that should also be fully reflected in the digital world.

The GDPR principles such as the one of data minimisation, purpose limitation and data protection by design and by default are applicable in this context and must be respected when digital identity systems are applied.

P. ¿Cuál es la relación entre la identidad digital y los últimos avances tecnológicos de innovación que utilizan inteligencia artificial?

Las tecnologías de IA pueden utilizarse tanto en beneficio como en detrimento de los derechos de las personas. Esta utilización para la autenticación requiere una evaluación cuidadosa de sus capacidades, limitaciones y riesgos derivados de sus características. Cuando la IA se utiliza en el contexto de la autenticación de identidad, no se puede subestimar la relevancia de la transparencia.

P. ¿Es necesaria la identificación digital en una sociedad hiperconectada? ¿Estamos respondiendo a una necesidad de la industria o a una necesidad del usuario/público?

Tener una o más identidades digitales es una necesidad reconocida desde hace mucho tiempo. La UE lleva más de dos décadas legislando sobre este tema. Mi país de origen, España, fue pionero en identidad digital y comenzó a proporcionar tarjetas de identificación electrónicas a todos los ciudadanos en 2006.

Los principios del GDPR tal como el de minimización de datos, limita la finalidad y la protección de datos por diseño y por defecto, y son aplicables en este contexto y deben respetarse cuando se aplican sistemas de identidad digital.

Maria Paz Canales

Global Policy Advisor at Derechos Digitales.
@MPaz_online

In a hyper-connected society, digital identity may overcome physical identity when that person interacts with private and public actors. The challenge explored by this session was how to enjoy the benefit of digital identity but preserving privacy and the respect for our fundamental rights.

Digital identity is made up of all the information that each person directly provides on the network, but also information from the digital trail that we leave on the internet from our searches of employment, social benefits, political preferences or consuming, which allows to generate specific profiles of ourselves quickly.

That information can be on the hands of digital services companies, or on government agencies who use that information to engage with the citizenship. There are also public-private partnerships in the provision of services that allow the transit of this information between private and public hands. In all these cases, digital Identity has become a must for all kind of digital interactions as a shortcut for efficiency to identify and serve a subject.

But unfortunately, more often than not, the deployment of digital identity systems is not accompanied of regulatory frameworks that protect privacy and other fundamental rights, such us non-discrimination, or there is lack of enforcement of the rules in place at the moment of design and deployment of those systems that account for a damage prevention. Digital identity has been captured in some way by a technosolucionist approach very spread in developing countries that perceive it as part of an "inevitable progress" without questioning its insertion context.

But digital identity initiatives in many cases imply legitimizing a differential surveillance towards people who find themselves in severe vulnerability conditions, depending on State assistance. In Latin America, for example, digital identity systems have been adopted in Venezuela for controlling access to essential goods; facial recognition have been used to control access to special benefits in transportation systems and access to educational institutions in Brazil; and Ecuador have been using biometric data to provide social benefits to children, aged persons and disable.

Usually, the risks of digital identification are downplayed in a double way. First, the diverse impact in traditionally vulnerable communities such as: aged persons, indigenous communities, non-binary people, women, and children that can have a more difficult access to digital identity technologies or being inadequately represented by the collected data. Second, digital Identity has evolved in risks as biometric technology has evolved: from fingerprints to facial or iris recognition. The risk of loosing control of our own identity in the hands of bad actors or to be discriminated in the access to services has become increasingly concrete and high in directly proportional way to the sophistication of data captured.

From the perspective of exercise of rights, digital identity has provided a narrative of erosion of privacy in exchange of a promised enhanced exercise of rights, either in the engagement with public services or in the profiling of consumers by private companies. The discourse behind seems to put privacy as a collateral damage for the benefits of being able to be uniquely identified and instantly satisfied according to the needs profiled.

The above is a false dilemma for a hyper-connected society. Digital identity infrastructure and services by big tech or States can be accompanied of democratic discussions that provide legitimacy to the systems among the population, particularly the traditionally marginalized, ensuring equity and inclusion. They should be designed and deployed according to legality, necessity, and proportionality principles to avoid harmful restriction of

rights exercise. And they must be designed to be accountable, for their legality and safety, providing remedy and alternative pathways to whoever suffer harm from the fail to be represented or adequately treated for the system.

La identidad digital está formada por toda la información que cada persona proporciona directamente en la red, pero también por la información de la huella digital que dejamos en internet a partir de nuestras búsquedas de empleo, prestaciones sociales, preferencias políticas o de consumo, que permite generar determinadas perfiles de nosotros mismos.

Lamentablemente, en la mayoría de los casos, el despliegue de sistemas de identidad digital no va acompañado de marcos normativos que protejan la privacidad y otros derechos fundamentales.

En América Latina, se han adoptado sistemas de identidad digital en Venezuela para controlar el acceso a bienes esenciales; En Brasil, el reconocimiento facial se ha utilizado para controlar el acceso a beneficios especiales en los sistemas de transporte y el acceso a instituciones educativas; y en Ecuador se han estado utilizando datos biométricos para brindar beneficios sociales a niños, ancianos y discapacitados.

Ulrich Kelber

The Federal Commissioner for Data Protection and Freedom of Information, Germany

Digital identities have always been an indispensable feature of internet commerce, digitisation of administrative services and of social media alike since the early days of the internet.

The way we know them, with distinct digital identities for every application, is, however, about to significantly change.

The rather fragmented landscape of small state ID schemes and corporate designed Log-In-Standards with varying degrees of trustworthiness and security might change to a significant degree.

This development seems to be the result of a push towards more digitization and of the attempt to generate economic growth by transforming government-citizen-relationships (E-Government) and business-consumer relationships. The risk of identity theft is supposed be reduced, trust increased by identifying people more reliably and overall convenience is said to be improved.

One factor of change are state-run ID schemes.

At the same time we see massive developments in the area of business-run Big Data and AI, which are globally considered key technologies for economic growth. They allow for multiple forms of identity verification in different settings, facial recognition in public spaces

is definitely one of the dark paths offered. And yes, we do have significant proof of inherent biases and discriminatory effects of a number of these systems.

Against this background it is my conviction that from our data protection perspective we need to reflect on these basic principles:

1. Anonymity still can be called an enormous achievement in many settings. Let's keep our public spaces in relative anonymity to foster public speech, the right to protest and to exercise our fundamental rights - even in a dawning age of the Internet of Things.

2. The use of biometrics is highly sensitive because of their often permanent nature. They stay with you for a lifetime, so the consequences of misuse can be extraordinarily detrimental to the individual. This is why systems of digital identity should avoid biometric data processing. Instead, there is a particular need for special justification.

3. Public digital identity schemes should remain voluntary. Making them mandatory, would negatively impact acceptance of digitization. Digital ID schemes should also not serve as a backdoor for government surveillance, but rather be clearly limited to their primary purposes.

4. The choice of identifiers for digital identities always matters. The necessity principle, in combination with the purpose-limitation-principle and data minimization considerations should guide the selection of and keep the number of identifiers at an absolute minimum.

5. Data Protection by Design plays the most prominent role in digital identities. It is our primary responsibility to foster the use of this principle within administrations and business, and supervise concrete applications with regard to compliance.

I believe that our forum provides an excellent opportunity for a conversation on digital identities and for deepening our understanding on the consequences of the recent changes in the set-up of digital identity schemes. I'm looking forward to our exchange and to hear from you what you think about this!

Desde los inicios de internet, las identidades digitales siempre han sido una característica indispensable del comercio en Internet, la digitalización de los servicios administrativos y de las redes sociales. Sin embargo, la forma en que los conocemos, con identidades digitales distintas para cada aplicación, está a punto de cambiar significativamente.

Este desarrollo parece ser el resultado de un impulso hacia una mayor digitalización y del intento de generar mayor crecimiento económico mediante la transformación de las relaciones Gobierno-ciudadano (gobierno electrónico) y las relaciones empresa-consumidor.

Este foro brinda una excelente oportunidad para una conversación sobre identidades digitales y para profundizar nuestra comprensión sobre las consecuencias de los cambios recientes en la configuración de los esquemas de identidad digital.

Digital Rights: Fostering Human Rights through technology

Nuhad Ponce

President Consejo Consultivo INAI, Mexico

I had the privilege to participate in GPA Assembly 2021. As we know in the digital age, and moreover with the Pandemic situation we suffered, we realized the needed and importance of having an update to the existing regulatory frameworks in our societies and countries.

It has become evident that the rights and guarantees to have as individuals the adequate protection to our personal data, personal and sensitive information, and cybersecurity of users who use digital services, are priority.

For this reason, when I was thinking in what will be necessary to protect human rights throughout technology, I realized that there are, all around the world, existing instruments that promote the defense and protection of digital rights that include, among others, access, use, and publication in digital media.

But do we as individuals, know this? Is this regulation enough? What do we need as societies to encourage the promotion of privacy protection with technological design perspective?

We know that the challenges are increasing, so it is essential to continue searching for an international legislation on this matter, so that we can be able to guarantee human rights in the digital age.

Como sabemos en la era digital, y más aún con la situación de la pandemia, nos dimos cuenta de la necesidad e importancia de tener una actualización de los marcos regulatorios existentes en nuestras sociedades y países.

Se ha hecho evidente que los derechos y garantías de tener como personas la protección adecuada a nuestros datos personales, información personal y sensible, y la ciberseguridad de los usuarios que hacen uso de los servicios digitales, son prioritarios.

Cuando pensamos en lo que será necesario para proteger los derechos humanos a través de la tecnología, surgen cuestionamientos tales como, ¿Qué necesitamos como sociedades para fomentar la promoción de la protección de la privacidad con la perspectiva del diseño tecnológico?

Sabemos que los desafíos son cada vez mayores, por lo que es fundamental es seguir buscando una legislación internacional en esta materia, para que podamos garantizar los derechos humanos en la era digital.

Gus Hosein

Executive Director at Privacy International

I want to start by saying that I was in Mexico ten years ago for this conference. I was asked when I was on a panel around big data because it was a topic that was still an innovation back then, if I felt like the law and regulation could help deal with the challenges of big data. I answered, much to the anger of the regulators in the room, that I didn't think that the regulators that were in the room were capable of dealing with that innovation question; that they were not going to stand up against big data and massive exploitation of data to the disadvantage of people across the world, and instead we would have to look to other regulators such as competition regulators. And in the last ten years, I think it's been proven right that competition regulators have stood up and said innovation should not happen with a new legal regime. Yet, we haven't seen that with data protection regulators, even where new laws have been introduced.

The whole idea that law can come in to save us from new threats and new challenges, I can say that as an organization that's been around for 25-30 years and that has been fighting intelligence agencies, fighting the googles and the facebooks, the problem hasn't been the law. The problem has been that our institutions, whether the courts or the regulatory authorities have not been willing to stand up and say they're going to stop something that's very problematic, legally and clearly in contravention to what is expected.

So, whenever we are approached to comment on: whether there should be a new convention? Should there be a new set of laws? Should there be a new set of safeguards? I always hesitate because the existing ones aren't enforced, the current regulators are being undermined, and I'm talking to an audience in Mexico from the United Kingdom, two regulatory regimes where regulators are being undermined. It is not just those two jurisdictions of course.

We are at this critical moment when our institutions have a poor track record, and we have a rule of law that is increasingly undermined, so to look for a new regime to solve our problems feels like a distraction.

Now to say something positive: an open global process of deliberation and debate could at least increase global awareness and concern about these innovations. It could make the industry and governments look out of step with peoples' concern. While that's never enough, it is often a good place to start.

Ante la idea de que la ley puede salvarnos de nuevas amenazas y nuevos desafíos, puedo decir que, como una organización que ha existido durante 25 a 30 años, y que ha estado luchando contra las agencias de inteligencia, el problema no ha sido la ley. El problema ha sido que nuestras instituciones que no han estado dispuestas a ponerse de pie y decir que van a detener algo que es muy problemático, y legalmente y claramente en contravención de lo que se espera.

Entonces, cada vez que me preguntan: ¿debería haber una nueva convención? ¿Debería haber un nuevo conjunto de leyes? ¿Debería haber un nuevo conjunto de salvaguardas de protección de datos personales? Siempre dudo porque los existentes no se cumplen y los reguladores actuales están siendo socavados.

Ahora, para decir algo positivo: un proceso global abierto de deliberación y debate podría al menos aumentar la conciencia y la preocupación global sobre estas innovaciones, ya que parecería que la industria y los gobiernos están fuera de sintonía con la preocupación de la gente. Si bien eso nunca es suficiente, a menudo es un buen lugar para comenzar.

Katitza Rodríguez

Policy Director for Global Privacy, Electronic Frontier Foundation

As Governments Seek Easier Access to Personal Information, Data Protection Authorities Can Play a Critical Role in Protecting Privacy and Human Rights

Today, I want to talk about a concerning trend in international cybercrime-fighting agreements that will (or threaten to) erode national legal privacy and other human rights safeguards in the name of facilitating law enforcement access to data across borders. Data Protection Authorities (DPAs) have a particularly important role to play by ensuring that data protection standards are strengthened, rather than eroded, during multilateral negotiations over these agreements.

Governments Are Ramping Up Pressure to Streamline Access to Data

Cross-border investigations raise difficult questions as widely varying legal systems clash. How do data protection laws regulate police collection and use of personal data when the collection process spans multiple jurisdictions and legal systems? More specifically, what kinds of legal safeguards derived from existing human rights and data protection toolkits will govern these and other forms of evidence collection across borders?

Governments have been ramping up pressure to streamline the process by which law enforcement in one country can get ahold of personal data abroad when it's relevant to an investigation —something that happens more and more frequently in our globalized world—.

A critical initiative on our radar comes from the Council of Europe (CoE) Cybercrime Committee (*not to be confused with the Convention 108 Data Protection Committee*). This

committee has recently finished negotiating the Second Additional Protocol to the Budapest Convention —an international agreement that deals with rules for police to access data across borders expected to be approved in November—.

The Second Protocol seeks to establish a new international standard that will govern several aspects of policing on a global scale in the future and sets out data protection safeguards in Article 14 that would apply to any transfer of personal data obtained through the protocol's new law enforcement powers, unless the transferring/receiving states have another agreement in place.

International Human Rights Standards Ignored

Article 14 requires parties to ensure that personal data collected through the Second Protocol's powers be used in a manner that is consistent with and relevant to the criminal investigative purposes that prompted its collection. However, contrary to most other data protection instruments, Article 14 data protection safeguards don't require all processing of personal data to be "adequate, fair, and proportionate" to its objective, a tenet of international human rights laws. Article 14's safeguards also don't require law enforcement data requests to be subject to entirely independent oversight.

Article 14 also prohibits parties from requiring the use of independent regulators (such as DPAs) to protect the privacy of personal data when transferred to other parties through the Second Protocol's investigative powers. Finally, Article 14 also outlines some safeguards for biometric data, but ultimately these are insufficient and undermine a growing international recognition that biometric data is sensitive and requires additional protection in all instances.

Taking a Stand for Robust Data Protection Standards

This is why we are calling for the Global Privacy Assembly to take up this topic and issue a resolution calling for more robust data protection standards in the context of cross-border policing powers: With detailed law enforcement powers should come detailed privacy and data protection safeguards, not a one-sided law enforcement compromise on privacy and data protection.

All these developments underscore the importance of finding ways to integrate and enforce human rights and data protection rules when governments seek access personal data. Solid red lines, limits, and standards should be established for accessing health, biometric, or other stored data held by tech companies that can be sought and used by law enforcement to track people's locations or monitor their activities.

Los gobiernos han aumentado la presión para agilizar el proceso mediante el cual las fuerzas del orden de un país pueden obtener datos personales en el extranjero cuando son relevantes para una investigación, algo que sucede cada vez con más frecuencia en nuestro mundo globalizado.

La iniciativa más reciente para esto proviene del Comité de Delitos Cibernéticos del Consejo de Europa (CoE) (que no debe confundirse con el Comité de Protección de Datos del Convenio 108) quien recientemente negoció el Segundo Protocolo Adicional a

la Convención de Budapest; un acuerdo internacional que establece las reglas para que la policía acceda a los datos a través de las fronteras.

Hacemos un llamado a la Asamblea Global de Privacidad para que emita una resolución que solicite estándares de protección de datos más sólidos en el contexto de los poderes policiales transfronterizos. Todos estos desarrollos subrayan la importancia de encontrar formas de integrar y hacer cumplir los derechos humanos y las normas de protección de datos cuando los gobiernos buscan acceder a datos personales.

Lorena Naranjo Godoy, Ph.D.

Director of the Master's Degree in Digital Law and Innovation with a mention in economics, trust, and digital transformation at UDLA and Leading Lawyer in the area of Digital Law and personal data protection at Spingarn S.A. Law Firm.

A culture of personal data protection is built through public policies as part of the responsibility of the State. However, private entities must also assume their role since they allow comprehensive compliance management and diffusers of the knowledge and training to achieve an approach to the subject. If each of us knows what to do with personal data from their specific functions in society, we will all be contributing in the long run to a society where data protection is worked from a comprehensive perspective.

People in the current State of society intrinsically have digital dignity, so their natural respect for this digital human being allows the recognition of the human right to personal data protection. There are two models in the world: the highest standard that places the person at the center and another that only views the person's privacy. That is, it is limited to sanctioning those acts that expose privacy and not all other forms of affectation associated with digital dignity. That reactive model is in crisis, so the balance has to be on the other side. It is the companies, organizations, and entities in general, as well as the State, that have to demonstrate that they comply with proper data management in such a way that it does not affect people, that is, to put people at the center, case.

On the contrary, the problem continues to be prolonged, whether with artificial intelligence, big data, or any other technology. This change in mentality from a reactive to a preventive model must occur through mechanisms such as Convention 108, through which a global standard can be established. Otherwise, another 30 years will pass, and this issue will continue to be treated as a local regulation, self-regulation, or ethics problem.

Just as when women's equality began to be talked about, it is necessary to raise awareness, educate children and adolescents, and train specialized professionals, that is, actions by the State, companies, academia, and organizations to jointly build a culture of personal data protection in a coordinated and coherent manner. This task is not easy or fast, but we have a history in other areas, and its good practices and recommendations can be replicated for the protection of personal data, digital rights, and digital human dignity.

Una cultura de protección de datos personales se construye a través de políticas públicas, como parte de la responsabilidad del Estado, sin embargo, también las entidades privadas deben asumir su rol. Si cada uno de nosotros sabe lo que tiene que hacer con los datos personales desde sus funciones específicas en la sociedad, todos estaremos contribuyendo a una sociedad en el que se trabaje la protección de datos desde una perspectiva integral.

Las personas en el estado actual de la sociedad, de forma intrínseca, tienen una dignidad digital, por lo que permite el reconocimiento del derecho humano a la protección de datos personales. Hay dos modelos en el mundo, uno, el estándar más alto que coloca a la persona en el centro, y el otro que visualiza únicamente la privacidad de la persona, es decir, se limita a sancionar aquellos actos que exponen la privacidad y no todas las otras formas de afectación asociadas a la dignidad digital.

Rafael Yuste

Professor at Columbia University

Let me start by presenting myself. I'm Rafael Yuste. I am a researcher at Columbia University, where I study how the brain works, and I'm also part of the Morningside group that in 2017 proposed new human rights, which we call "neural rights or brain rights," to be added to the Universal Declaration or to existing UN Treaties of Human Rights.

We propose these rights are needed because technology, particularly neurotechnology, is advancing quickly and is not regulated. Neurotechnology can affect the essence of what it means to be human. Neurotechnology are techniques, methods, and tools to record the activity of neurons in the brain or to change the activity of neurons in the brain. Because the brain is not just another organ, but it is the organ that generates the human mind, the ability to record the activity of the brain and to change the activity of the brain makes it possible to decode the activity of the mind and to change the activity of the mind. Humans define ourselves by our mental abilities and by our minds, so this is the first time in history that technology can have access to our cognitive processes. The brain should be protected with these new human rights.

The neural rights that we proposed are five:

1. The right to our mental privacy so that the contents of your brain activity cannot be decoded without our consent.

2. The right to our identity, to our own self, is necessary because, with neurotechnology, one could change the sense of self.

3. The right to our own agency, that means to our free will, to protect our decision-making without interference.

4. The right to fair access to mental and cognitive augmentation is related to the possibility that neurotechnology will lead to mental and cognitive augmentation by introducing brain-computer interfaces that connect our brains to external databases, external artificial intelligence, supercomputers, or the entire internet.

5. The final neural right is protection from algorithmic bias.

Let me give some examples of how these rights are becoming part of our lives. In Chile, a constitutional amendment was approved that makes cerebral integrity a fundamental human right, as well as a bill of law of neural protection incorporating these five neural rights into the Chilean legislation. In Spain, the secretary of State for Artificial Intelligence has released a charter of digital rights which also covers neural rights. The last example is the United Nations, which also has interested in neural rights. In the common agenda for the UN for the next six years, you will see that it mentions that the Universal Declaration of Human Rights needs updating.

Soy Rafael Yuste y soy parte del grupo Morningside que en 2017 propuso nuevos derechos humanos, a los que llamamos "neuroderechos", para agregarlos a la Declaración Universal de Derechos Humanos de la ONU.

Los derechos neuronales que proponemos son cinco:

1. El derecho a nuestra privacidad mental para que los contenidos de nuestra actividad cerebral no puedan ser decodificados sin nuestro consentimiento.

2. El derecho a nuestra identidad, a nuestro propio yo, es necesario porque con la neurotecnología podría cambiar el sentido de uno mismo.

3. El derecho a nuestra propia agencia, es decir, a nuestro libre albedrío, para proteger nuestra toma de decisiones sin interferencias.

4. El derecho a un acceso justo al aumento mental y cognitivo, el cual está relacionado con la posibilidad de que la neurotecnología introduzca interfaces cerebro-computadora que conectan nuestros cerebros con bases de datos externas, inteligencia artificial externa, supercomputadoras y/o todo el Internet.

5. El último es el derecho neuronal para la protección contra el sesgo algorítmico.

Invited Contributions

Alexander White

Privacy Commissioner for Bermuda

The theme of our 2021 session, "A human centric approach," resonated through each report of the excellent work by the GPA's various Working Groups. The past few years have shown that decisions about privacy and data protection have a real-world, human impact. That reality was made even more clear by the need to use data and personal information in response to the Covid-19 pandemic. The Covid-19 Temporary Working Group proved the value of the GPA and of our collective efforts. As each GPA member worked with our local governments to respond to public health circumstances, we could turn to an invaluable resource to inform the work.

Similarly, we as a global community agreed that not only should data be prohibited from causing harm, but it can and should also be used for good —and for the public good—. To do so while effectively protecting the rights of individuals, we must move with care and forethought. For this reason and others, our office was proud to co-sponsor the resolution on the GPA Strategic Plan 2021-2023. In order to enable effective change in our global society, we as a community of regulators much make our priorities clear. The strategic plan established clear policy focus areas that will help political and community leaders understand important human centric issues affecting data sharing and technology.

On a personal level, the 43rd session of the Global Privacy Assembly will always hold a special place in my heart as the event in which our colleagues selected our office to be a future host of the occasion. As a relatively young data protection authority, we are honoured by the trust shown by the global community, and by the opportunity to contribute on the GPA's Executive Committee.

El tema central del 2021, "Un enfoque centrado en el ser humano", resonó en cada informe de los grupos de trabajo de la GPA. Los últimos años han demostrado que las decisiones sobre privacidad y protección de datos tienen un impacto humano en el mundo real.

Nosotros, como comunidad global, acordamos que no solo se debe prohibir que los datos causen daño, sino que también pueden y deben usarse para el bien, y para el bien público.

A nivel personal, la 43.ª sesión de la GPA ocupa un lugar especial en mi corazón, como el evento en el que nuestros colegas seleccionaron a nuestra institución para ser el futuro anfitrión de la conferencia en el 2023. Como una autoridad de protección de datos relativamente joven, nos sentimos honrados por la confianza mostrada y por la oportunidad de contribuir con el Comité Ejecutivo de la organización.

Ana Brian Nougrères

United Nations Special Rapporteur on the right to privacy

The doctrine that protects the protection of personal data is a consequence of the growing concern about the advancement of information and communication technologies, which provides the possibility of managing and increasingly manipulating information, either by States as well as large organizations, with great potential risk to attack the freedom, life, and dignity of people.

The data undeniably became an input for production and came to have a transcendent value from both the social point of view and the economic point of view.

We are in a moment of transformation, which began to be conceived with the considerable increase in bandwidth, the widespread use of smart mobile devices, and the use of social networks, and continued to evolve disruptively with 3D printing, augmented reality, artificial intelligence, nanotechnology, and robotics.

The fundamental human right to the protection of personal data protects people insofar as it protects the data of which they are owners. This data is part of their being, generating the right to informational self-determination, according to which each person has the right to dispose their data freely and autonomously.

The protection of personal data, for its part, enables other rights such as the right to freedom of information, dignity, free expression, freedom of opinion, dissemination of thought, and freedom of investigation, among many others. Thus, it constitutes a transcendent tool to guarantee the exercise of other civil and political, economic, social, and cultural rights since it operates transversally and helps us to calibrate the democratic state of the people.

Now, concerning the qualitative development of privacy principles and their global application and, more specifically, the practical realization of the right to personal data protection, once enshrined in regulations, it is necessary to note the need to channel ways for awareness and education in the matter, adapting ourselves multiculturally to each situation.

Working on the concept of privacy and protection of personal data as values that enhance democracy opens us to the potential of educating the different social actors, always respecting diversity, which also implies educating in human rights.

Our proposal, as the United Nations Special Rapporteur on Privacy, is in the sense of generating instances of work in groups, implemented horizontally and multisectoral to work closer to a world in which privacy and the protection of personal data march harmoniously towards a global context structured based on mutual respect and agreed on principles. Always bearing in mind that the entire human rights system is nothing more than a tool for the good of the human person, which must be our objective and the goal of our efforts.

La doctrina que ampara la protección de datos personales es consecuencia de la creciente preocupación por el avance de las tecnologías de la información y de las comunicaciones. Los datos pasaron a ser innegablemente un insumo para la producción al tener un valor trascendente desde el punto de vista social y económico.

Nuestra propuesta, como Relatora Especial de las Naciones Unidas en materia de Privacidad, es en el sentido de generar instancias de trabajo en grupos, implementadas horizontal y multisectorialmente, con la finalidad de trabajar para acercarnos a un mundo en el cual la privacidad y la protección de datos personales marchen armónicamente hacia un contexto global estructurado con base en respetos mutuos y principios consensuados; teniendo en consideración siempre que todo el sistema de derechos humanos no es más que una herramienta para el bien de la persona humana, que debe ser nuestro objeto y el fin último de nuestros esfuerzos.

Angelene Falk

Australian Information Commissioner and Privacy Commissioner, Chair of the GPA SDSC and GPA Executive Committee Member

As we near the conclusion of this wonderful event, the 43rd Global Privacy Assembly conference made possible by our host INAI, I would like to take this opportunity on behalf of the Executive Committee, to recognise and appreciate the contribution of the outgoing GPA chair, Commissioner Elizabeth Denham.

Each chair offers a unique contribution. Commissioner Denham has served 2 terms and 3 years as chair, leading through a time of transition, evolution and of global challenge.

I recall the meeting of Executive Committee in London in 2019. We met to develop the draft Strategic Plan 2019–21, and I remember Commissioner Denham challenging us to be ambitious. In Albania, chair, you led the adoption of that ambitious strategic plan, a set of strategic priorities and the policy strategy that strengthened the group's position as an effective and influential international forum. Our new GPA name and logo followed, developed by INAI, reflecting our modernisation as a group that supports one another year-round, sharing knowledge and building stronger cooperation.

You have modelled the 4 attributes represented in our GPA logo: international cooperation, knowledge sharing, independence and leadership.

The values you have held true to have strengthened our foundations. The value of the GPA being as diverse as the world we seek to influence, as you put it so well yesterday. The value of the contributions of all.

We have witnessed those values in action, in the inclusive way in which you have chaired the last 3 conferences. You masterfully chair to ensure the voices of all are heard. You have moderated, presented and provided insights. We have all benefited from the depth

and breadth of your experience, that you have generously contributed over the course of this conference and always.

You are a chair based in Europe, but of North American background. This connects well with the message that is at the heart of the GPA: that wherever we are around the globe, what connects us is the unity we have in our vision and mission to work towards a global regulatory environment with clear and consistently high standards of data protection.

We have been inspired and motivated by your personal commitment and determination to unite us behind this common purpose for global citizens around the world.

You have set the assembly on a clear course of continued evolution: to focus on what matters to our citizens. We know you see the huge potential in the GPA to work together to build its voice and impact. We have our new strategic plan building on these strong foundations to maximise the voice and impact of the assembly to advance global privacy in this accelerated age of digitisation.

But I can't conclude without also highlighting the unique circumstances of your tenure through the global pandemic. You have led the assembly during a time of incredible challenge: you stepped forward and called out common challenges for all GPA members, and assisted the GPA to address them through our common effort.

The Executive Committee recognises the outstanding leadership of Chair Elizabeth Denham, whose vision and commitment has resulted in the evolution of the GPA to become a global voice, and a strategic body, that supports members year round, to effectively fulfil their mandates, both individually and in concert, through a time of unprecedented global challenge. With our greatest appreciation.

Quisiera aprovechar esta oportunidad, en nombre del Comité Ejecutivo de la GPA, para reconocer y agradecer a la presidenta saliente, la comisionada Elizabeth Denham, quien ha destacado en todo momento nuestro lema de la GPA: cooperación internacional, intercambio de conocimientos, independencia y liderazgo.

Ha sido una presidenta con sede en Europa, pero de origen norteamericano. Lo que se relaciona con el lema en el corazón de la GPA: dondequiera que estemos alrededor del mundo, lo que nos conecta es la unidad que tenemos en nuestra visión y misión para trabajar hacia un entorno regulatorio global con estándares claros y altos de protección de datos personales.

El Comité Ejecutivo reconoce el destacado liderazgo de la Presidenta Denham, cuya visión y compromiso han resultado en la evolución de la Asamblea Global de Privacidad para convertirse en una voz global y en un organismo estratégico que apoya a los miembros durante todo el año para cumplir con eficacia sus mandatos, tanto individualmente como en conjunto, sobre todo en una época de desafíos globales sin precedentes.

Beatriz de Anchorena

Director of the Access to Public Information Agency, Argentina

In the last years, there has been an exponential growth in the use of technology to carry out daily activities, more so by the pandemic. Thus, the Agency has developed a series of recommendations on how to face those challenges safely, accompanied the citizens, and guaranteed their access to rights

As the first female Director of the Agency of Access to Public Information I shared the outlook, principles, and strategic pillars on which we plan to work as an Agency in the following five years to promote and develop tools in line with today's challenges and to promote an agile and intelligent State close to its citizens.

The State needs to ensure that society can take advantage of the benefits of innovation while avoiding negative consequences on the data subjects' welfare and general interest. The protection of personal data is inherent to the right of honor and dignity of individuals and, therefore, developing standards, fomenting data protection and privacy culture is imperative to respect and guarantee their rights. This needs to be done with a human centric approach, taking a step towards ensuring that the data subject is placed in a central position and has full power over their personal data. In this sense, the Agency considers data subjects to be empowered actors in the management of their personal lives including their data and, as such, they are the core of personal data protection regulation. Therefore, it is important to remember that data subjects are the rights-holders of a series of rights regarding data.

Thus, moving forward, the intention is to place the matter of data protection at the forefront of the national agenda to empower citizens in their rights regarding personal data by furthering the level of information on data protection and its regulation. In addition, we must consider the Agency as the engine of development, placed strongly at the center and deploying its state capacities to promote interaction with the different sectors of society, ensuring that all obliged subjects have the tools and devices to concretise, materialise and watch over the protection of personal data.

Moreover, the Agency recognizes the importance of international cooperation to face the challenges regarding the protection of personal data, and thus it has increased its active participation in various organizations such as the Global Privacy Assembly and the Red Iberoamericana de Protección de Datos with the aim to promote the protection of personal data with a human centric approach.

Como la primera mujer Directora de la Agencia de Acceso a la Información Pública de Argentina, compartí la mirada, los principios y los pilares estratégicos sobre los que planeamos trabajar en los próximos cinco años para promover y desarrollar herra-

mientas acordes a los desafíos actuales y promover un Estado ágil e inteligente cercano a sus ciudadanos.

El Estado debe garantizar que la sociedad pueda aprovechar los beneficios de la innovación tecnológica, evitando consecuencias negativas para el bienestar y el interés general de los interesados. La protección de datos personales es inherente al derecho, al honor, y a la dignidad de las personas, por lo que desarrollar normas, fomentar la cultura de la protección de datos y la privacidad es imperativo para respetar y garantizar sus derechos; todo con un enfoque centrado en el ser humano.

Así mismo, la Agencia reconoce la importancia de la cooperación internacional para enfrentar los desafíos en materia de protección de datos personales.

Brent R Homan

Deputy Commissioner, Office of the Privacy Commissioner of Canada. Co-Chair of IEWG and DCCWG

Regulatory Enforcement Cooperation as a human-centric approach to Privacy and Data Protection

From a regulatory posture, a human-centric approach is one that seeks to understand and ultimately serve the best interests of individuals in the most effective and impactful way. And in the privacy realm, a human-centric approach is of elevated priority given that privacy rights also represent a prerequisite for the advancement of other human rights and the preservation of democratic values.

Today's global societies and economies have evolved exponentially towards an unprecedented state of connectedness and digitization. The personal information of the worlds' citizenry is the key driver to innumerable social and commercial platforms, with the lines of such digital platforms brackishly blurring and overlapping. It is against this environmental backdrop, that regulatory cooperation has never been more essential to optimizing the protection of individuals' data and privacy rights. And we have witnessed this first-hand at the GPA through our leadership activities in both the International Enforcement Working Group (IEWG) and the Digital Citizen and Consumer Working Group (DCCWG).

Within the privacy and data-protection realm we have seen how the greatest privacy risks are shared by jurisdictions all over the world, and that often the most effective means of addressing such common risks is through collaboration. To illustrate, with the onset of the global pandemic in 2020, IEWG members acted swiftly to address Video-Conferencing Technology (VCT) risks through a joint enforcement action that resulted in the elevation of privacy protections for VCT platforms to the collective benefit of citizens around the world.

Across Regulatory Spheres we have seen through the work of the DCCWG how privacy issues can also represent consumer protection and competition issues (and vice versa), and how actions taken by an authority in one regulatory sphere can have either a complementary or disruptive impact on an individual's rights and protections in another regulatory

sphere. The solution championed by the DCCWG is elegant and simple– *cross-regulatory cooperation* where authorities, working together, can amplify the complements and mitigate the tensions towards ensuring a more holistic protection of individuals' privacy and consumer protection rights. Examples of such human-centric initiatives and outcomes abound in the DCCWG's Annual Report.

Whether regulatory collaboration is of a horizontal or vertical pedigree, its merits as a human-centric endeavor are clear: It can produce the most effective and all-encompassing of protections to our collective global citizenry, given the commonality of privacy risks internationally, and the increasing incidence of such risks also intersecting with other regulatory harms (e.g. from anti-competitive behavior).

It has become an axiom that through collaboration the global regulatory community *expands its collective capacity to take action and amplifies the impact of those actions*. And to that end, members of the IEWG and DCCWG are proud to carry the flag and champion the merits of collaboration to the world on behalf of the GPA.

Desde una visión regulatoria, un enfoque centrado en el ser humano es aquel que busca comprender y, en última instancia, servir a los mejores intereses de las personas de la manera más efectiva e impactante. Y en el ámbito de la privacidad, un enfoque centrado en el ser humano es de alta prioridad, dado que los derechos de privacidad también representan un requisito previo para el avance de otros derechos humanos y la preservación de los valores democráticos.

La cooperación regulatoria nunca ha sido más esencial para optimizar la protección de los datos personales y los derechos de privacidad de las personas, pues hemos sido testigos de esto de primera mano a través de nuestras actividades de liderazgo, tanto en el Grupo de Trabajo de Cumplimiento Internacional (IEWG) como en el Grupo de Trabajo de Consumidores y Ciudadanos Digitales (DCCWG) de la GPA.

Como miembros del IEWG y del DCCWG nos enorgullecemos de defender los méritos de la colaboración ante el mundo en nombre de la GPA.

Catherine Lennman

Swiss Data Protection Authority and Chair of the GPA WG AID

The Working Group on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis management (the WG AID) was established in 2020 by the Resolution on the Role of Personal Data Protection in International Development Aid, International Humanitarian Aid and Crisis management during the 42nd GPA. The work of the WG AID mainly focuses on the advancement of privacy protection worldwide, the promotion of high data protection standards as stated in the GPA's Strategic Direction (2021-23).

Over the years, the WG AID has strengthened its presence with relevant actors at both the bilateral and multilateral levels and has thus maximized the reach of the GPA's voice by strengthening the relations with the actors of international development aid and humanitarian aid. All these actions have been undertaken to contribute to building a global privacy community committed to high standards of protection for individuals, particularly for those who are beneficiaries of international development or humanitarian aid programmes and who are particularly vulnerable.

Personal data protection is of fundamental importance for humanitarian and development aid organizations as it is an integral part of protecting the life, integrity and dignity of their beneficiaries.

Working on this topic has shown me how data protection can be a life and death matter. For example, the misuse of data vulnerable individuals in a refugee camp may affect not only their privacy rights but also their very existence! It is right that our international assembly offers support to the crucial role that those actors play. We will continue to demonstrates that data protection legislation does not prohibit the collection and sharing of personal data, but rather provides the framework in which personal data can be used in the knowledge and confidence that individuals' right to privacy is respected.

Finally, I have learned that data protection is an enabler to some core humanitarian values and principles. For example, it is a key tool to be people centric, which means keeping the individual at the centre and ensuring that they can exercise their rights. It is also a central element of accountability to affected population in so far as it involves handling people's data or running these activities according to clearly defined principles, policies and rules and being accountable to such individuals.

La protección de datos personales es fundamental para las organizaciones humanitarias y de ayuda al desarrollo, ya que es parte integral de la protección de la vida, la integridad y la dignidad de sus beneficiarios. Incluso puede ser un asunto de vida o muerte. El uso indebido de datos de personas vulnerables en un campo de refugiados puede afectar no solo sus derechos de privacidad sino también su propia existencia.

Continuaremos demostrando que la legislación de protección de datos no prohíbe la recopilación y el intercambio de datos personales, sino que proporciona el marco en el que los datos pueden utilizarse con el conocimiento y la confianza de que se respete el derecho a la privacidad de las personas.

La protección de datos es un habilitador de algunos valores y principios humanitarios al ser una herramienta clave centrada en las personas. También es un elemento de rendición de cuentas a la población afectada en la medida en que implica manejar los datos de las personas o ejecutar estas actividades de acuerdo con principios, políticas y reglas definidas.

Faruk Bilir

President of the Personal Data Protection Authority of Turkey ('KVKK')

Each innovation that facilitates human life and serves the humankind is exciting. The important point here is that innovative initiatives and new technologies should be handled in an understanding that respects human rights, considering the value given for the protection of human dignity.

Protection of personal data, as one of the mechanisms to protect human rights, also aims to ensure that personal data is processed for legitimate purposes and means. New challenges posed to privacy due to emerging technologies are the starting point of the specific regulations on protection of personal data. Accordingly, in many countries, protection of personal data is guaranteed by legal regulations. However, it is also certain that there will be differences in approach on how to ensure the protection of this data. It is accomplishable to meet on a common ground on a global scale to protect the privacy of individuals. Of all the common grounds, the most inclusive and applicable one is the adoption of a human-centric approach in the protection of personal data.

Sustainable solutions are needed to ensure that the protection of personal data, which has a dynamic structure, does not lose its functionality. In fact, non-human-centric approaches to the protection of personal data will not be sustainable in the long term.

Humanity is moving towards to a new era where the boundaries between the physical and digital worlds begin to transform into a hybrid reality. This transformation, in which digital technologies play a leading role, causes a paradigm shift in terms of right to privacy and protection of personal data. The advancement of technologies, such as 'artificial intelligence', that can create value from data, and technologies such as 'metaverse' raises the necessity to introduce new perspectives on data protection.

Change seems impossible until it happens. Once it happens, it seems inevitable. Thus, in order to achieve a technology-privacy balance, we should be prepared for sudden technological changes and transformations, and a proactive and human-oriented approach should be the basis for data protection. Ethics can assist the law at this point. Therefore, the law and ethics can be seen as activators of a human-centric approach. Ethical initiatives are great assets in respect of being a supporter or a complement to existing legal regulations.

The necessity of preserving privacy of individuals emerges as the unchanging truth in a changing world. The basis of privacy is the autonomy of individuals and their power to make decisions about their own future. The autonomy of the individual is intimately linked to what degree the data protection policies human-centered will be in the future.

Therefore, technology should be designed in such a way that it preserves privacy. In this framework, while the positive potential of algorithmic decision making is recognized, ways to eliminate the risks or possible negative consequences on individuals should be sought at the same time.

Another notable issue here is preventing biases and discrimination by implementing transparent and accountable algorithms during their development. Transparency is a key principle to identify and address discrimination in this regard, which also facilitates the accountability. Transparency actually enables individuals to have more control over their own data. For this reason, the notion of "staying human in the digital age" should be idealized and placed at the center of technological developments in the field of personal data protection.

The next quarter century is predicted to see some technological developments that will affect the future of humanity for perhaps three centuries.

So, in the future, will we manage our data, or will our data manage us? The answer to this question will be determined by 'human'.

La protección de los datos personales, como uno de los mecanismos para proteger los derechos humanos, tiene como objetivo garantizar que estos sean tratados para fines y medios legítimos. Los nuevos retos que plantean las tecnologías emergentes son el punto de partida de la normativa de la privacidad, la cual debe reunirse en un punto común de escala mundial para lograr su efectiva protección. Esta adopción deber hacerse desde un enfoque centrado en el ser humano.

Debemos estar preparados para cambios y transformaciones tecnológicas, y un enfoque proactivo y orientado al ser humano debe ser la base para la protección de los datos personales.

Se predice que el próximo cuarto de siglo tendrá desarrollos tecnológicos que afectarán el futuro de la humanidad durante quizás tres siglos. Entonces, en el futuro, ¿administraremos nuestros datos o nuestros datos nos administrarán a nosotros? La respuesta a esta pregunta será determinada por el 'humano'.

Marie-Laure Denis

Chair of the GPA Digital Education Working Group CNIL, France

The accelerated digitalisation of our society is increasingly placing the protection of personal data at the heart of legal, economic and political issues. Everyone, in his or her own sphere of action, has to find a balance between the protection of privacy and often diverging interests, with the particularity that the regulations concerned, both in Europe with the GDPR and in the global legal landscape, place the individual and his or her rights at the centre of the model.

This human-centric approach is particularly illustrated by the emergence of the right to be forgotten, which enables people to take back control of their digital life according to their own choices and needs.

In this respect, it should be noted that most of the de-listing requests are made by "ordinary" citizens, including a large number of young people. By doing so, they seek to remove themselves from an excessive Internet footprint and to give a "fair image of themselves".

Digital education and data protection are therefore a key issue that should be addressed not only by regulators, but also by governments, educational authorities, civil society and the private sector. This is the only way to create a trusted digital environment.

The work carried out by the Global Privacy Assembly (GPA) is a direct contribution to this collective ambition. In this respect, the Digital Education Working Group which I have the privilege to chair adopted several resolutions in this area. Referring to the most recent resolution on children's digital rights (2021, Mexico), it precisely aims to strengthen their information on online services and to guarantee the effectiveness of their digital rights.

Giving priority to education is an essential prerequisite for building a digital society that respects our common human values.

El enfoque centrado en el ser humano está relacionado con el derecho al olvido, que permite a las personas recuperar el control de su vida digital de acuerdo con sus propias elecciones y necesidades. Para esto, la educación digital y la protección de datos personales son clave para que no solo las autoridades reguladoras, sino también los gobiernos, las instituciones educativas, la sociedad civil y el sector privado creen un entorno digital de confianza.

El trabajo realizado por la Asamblea Global de Privacidad es una contribución directa a esta ambición colectiva. El Grupo de Trabajo de Educación Digital, que tengo el privilegio de presidir, adoptó varias resoluciones en este ámbito. Hago referencia a la más reciente resolución sobre los derechos digitales de la niñez (2021, México) la cual tiene como objetivo fortalecer su información en los servicios en línea y garantizar la efectividad de sus derechos digitales.

Dar prioridad a la educación es un requisito esencial para construir una sociedad digital que respete nuestros valores humanos.

Paula Hothersall

Director of International Regulatory Cooperation at ICO, UK

• Thank you for the opportunity to share some of the work that the GPA Working Group Global frameworks and standards has delivered this year.

• One of our main allocated actions in the policy strategy was to deliver an analysis of global privacy and data protection frameworks. This was completed and adopted in 2020. The analysis was the first of its kind and covered ten global frameworks: the GPA Madrid Resolution; OECD Privacy Guidelines; APEC Privacy Framework; C108; C108+; Ibero-American Standards; African Union Convention; ECOWAS supplementary act; EU GDPR; UN Guidelines.

• The analysis found a high degree of commonality between the frameworks, especially in relation to key principles and some core rights. It suggested a commitment to shared values between the frameworks and the GPA members who work within them, and our intention was that the analysis would provide a point of reference for GPA members to

use in conversations with those they regulate, their governments and wider stakeholders, and that it could in turn help to promote clear and consistently high standards across the globe.

• This year, we have heard positive reports of how the global frameworks analysis has been used as a reference by both external organisations and GPA members, and is positively influencing privacy and data protection standards in a variety of ways, from GPA members using it as reference material when preparing responses to their governments' consultations, to the analysis being referenced in European Data Protection Board's Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, where it is recommended as a resource for data controllers to assess a third country for suitability for data transfers from the EU.

• Our focus in 2021 has been to build on that analysis work – to build on the commonalities we found by drawing out key principles on several more specific topics such as government access to personal data, and the independence of privacy and data protection authorities. We also worked on further analysis of cross border transfer mechanisms, and on developing agreed meanings of key data protection terms.

• The topic of cross border data transfers is a key area of interest to many countries and organisations, both within and outside the privacy and data protection community. Building on last year's analysis which touched on cross border transfers, the working group undertook research on the various mechanisms in use, and surveyed GPA members on mechanisms used in their jurisdictions. Overall commonality was identified between the mechanisms in the various frameworks, representing a relatively consistent set of tools that can be used to transfer personal data. This could be of use to jurisdictions yet to implement a transfers framework, or a privacy and data protection framework in general, to develop one that aligns with other global approaches. We're also keen to build further on this work in a way that's relevant to the wider world – so we've asked the GPA Reference Panel to review the report and advise us on possible ways to take it forward.

• Finally, we considered the data protection terms found in the frameworks analysed —if we want to achieve clear and consistently high standards of data protection worldwide, we have to be clear about what we mean—. We analysed the use of key terms across the frameworks, and developed a first set of terms and their meanings. We'll continue this with more terms next year.

Agradezco la oportunidad de compartir parte de las actividades que el grupo de trabajo de la GPA Global frameworks and standards ha realizado:

• En el 2020 una de nuestras principales acciones fue entregar un análisis de los marcos globales de privacidad y protección de datos. Nuestra intención con este análisis fue proporcionar un punto de referencia para que los miembros de la GPA lo puedan usar en conversaciones con quienes regulan sus gobiernos y partes interesadas, y que, a su vez, ayude a promover estándares claros y consistentes en todo el mundo.

• Nuestro enfoque en 2021 se centró en construir, basados en este análisis, los principios clave sobre varios temas en específicos, como el acceso del gobierno a los datos personales y la independencia de las autoridades de privacidad y protección de datos, así como los mecanismos de transferencia transfronteriza.

• Finalmente, si queremos lograr estándares de protección de datos en todo el mundo, debemos tener claro lo que queremos decir, por lo que analizamos el uso de términos clave en los marcos y desarrollamos un primer conjunto de términos y sus significados. Continuaremos con más términos el próximo año.

Third part

Former GPA Secretariat ICO, UK

The GPA Secretariat from the UK Information Commissioner's Office was responsible for administering all of the GPA's work between 2018-2021. The Secretariat stepped down in October 2021 to hand over to a new Chair/Secretariat Host Authority (Mexico's Member Authority, the INAI).

The Secretariat wishes to send a special final message to the 43rd GPA Hosts at INAI and the GPA Membership, thanking you for your involvement in GPA activities surrounding the 43rd GPA conference.

We'd also like to thank for everyone's contribution to the regular GPA Newsletters which have evolved to become a remarkable vehicle for the GPA Voice in the last three years, but also showcasing our Assembly's richness of diversity in line with the conference's strategic priorities.

We couldn't have done it without you! Thank you!

Current GPA Secretariat INAI, Mexico

Laura Sofia Gómez Madrigal

On behalf of the Plenary of the National Institute for Transparency, Access to Information, and Personal Data Protection of México, as Chair and secretariat of the Global Privacy Assembly (GPA), we wish to convey our upmost gratitude to all of you, for participating as chairs, moderators, and speakers at the 43rd Global Privacy Assembly.

Your participation embodied an outstanding opportunity to highlight the value of multilateral relations and actions towards data protection. We are very thankful to the past Secretariat, the Information Commissioner's Office of the United Kingdom for their continuous support during what was —due to its virtual nature— a uniquely challenging process.

This compilation of your participation at the 43rd Global Privacy Assembly represents key moments in our commitment to dialogue and continuous learning and bears witness to the road we have travelled and points the way to the journey still ahead of us.

The reflections shared promise a more inclusive, sustainable, and equitable future and have confirmed that the proper protection of privacy and personal data, requires strong and effective regulatory and institutional frameworks.

Undoubtedly, all the contributions included herein represent a valuable opportunity to strengthen the culture of personal data protection at the national and international level.

We also express our gratefulness to all the authorities and public in general who participated in this forum, which represents a significant step in favor of privacy and personal data protection.

Vitelio Ruiz Bernal

The evolution of the right privacy and to the protection of personal data has been steady since the creation of its first concepts by Warren and Brandeis. Also, it is important to recognize that in the last 15 years its advancement and recognition across the globe has been of enormous proportions and it keeps growing as more and more countries start to legislate this human right in their own jurisdictions.

In the globalized world that we inhabit the international personal data transfers, seems to be something of need for the trade and growth of the economies, and therefore supposes

a challenge for the data protection authorities, as every authority has its own law and its own understanding in some cases of concepts. The goal for every data protection authority is the same, how to guarantee the protection of this right with an adequate level of measures and safeguards that guarantee that this protection remains the same without regarding the jurisdiction and without stalling the operations and economies across the globe.

To achieve this common goal, it is necessary to explore what we have in common between our authorities, laws, and concepts. The normative convergence is something that seems ideal to collaborate in many ways but mostly to be able to guarantee this human rights. The dialogues, exchanges of ideas and discussions to accomplish the normative convergence are in the essence of the GPA.

Daniela Reyes Torres

The year 2021 was marked by society's flexibility and resilience to respond to the health, technological, economic, political, and social conditions presented worldwide. Given this scenario, the Global Privacy Assembly positioned itself as a cutting-edge forum and a world reference in the right to privacy and the protection of personal data.

We are convinced that the GPA is a compelling organization capable of maintaining an open dialogue between data protection authorities to achieve a normative convergence that will benefit the people worldwide. There is a need to base any discussions with a human center approach, as it is the only view that will let us understand people's needs, motivations, and concerns. To consider the human factors means considering the human needs, capacities, perceptions, and culture that will allow to better implement privacy and data protection public policies and initiatives.

As part of the INAI team working in the Global Privacy Assembly for the last years, we want to thank every member, observer, and key partner which whom we have had and still have the pleasure of working.

"Cooperation is the thorough conviction that nobody can get there unless everybody gets there".

Virginia Burden

INAI Commissioners, Mexico

As we have read through the voices of experts in data protection and privacy, the 43rd Global Privacy Assembly has allowed us to reflect that the use of new technologies must be guided by a human-center approach based on the liberty of expression and the right to privacy, to avoid damage to the integrity of people. There is a necessity for regulators, companies, and citizens to privilege in their agendas the protection and security of personal information that circulates without restrictions in the digital age.

This Assembly allowed Mexico to position human rights, especially the protection of privacy, as a tool that guarantees free access to knowledge, empowering the country in a global, safe, responsible, and united scenario.

The progress of digital transformation is irreversible, and the health pandemic has shown the need to reduce digital gaps by using new technologies to build a future of economic growth, job creation, inequality reduction, and greater sustainability.

Rapid technological evolution and globalization have posed new challenges for data management. The magnitude of the exchange of personal data has increased significantly, allowing the transmission of data on an unprecedented scale and globally decentralized manner. From a sustainable and inclusive perspective, the importance of digital rights represents a turning point towards a society increasingly and rapidly oriented toward the exchange of cross-border data flows that foster the normative development of international standards for the adequate protection of human rights.

The authorities safeguarding personal data protection have recognized in this Assembly the challenges that we have faced during the last two years regarding the increased demand for information by the public and private sectors. It becomes imminent that all the actors involved work in a coordinated manner to build mechanisms that allow the secure exchange of information at a national and international level.

There is a consensus on the need to work on normative convergence to promote the digital economy, particularly in consumer protection, personal data protection, identity, payments and digital values, transport and logistics standards, and tax regimes.

For the adequate protection of personal data, it is necessary to have international standards where a common language is spoken that allow the adoption of similar principles and provisions that help guarantee the adequate protection of personal data protection and privacy. This is under three foundations

• building on the work that already exists,

• respecting cultures, and

• keeping in mind the value of privacy.

We must ask ourselves if we are using the technologies of the Fourth Industrial Revolution for the society we want to live in. Who decides how we want this to be? We need collective reflections based on the principle that human dignity is respected.

As a community, we must keep up the pace if we want to be able to protect people's right to privacy, putting them at the center of the discussion to know and understand what they feel.

In Mexico, protecting personal data and privacy is a fundamental right. With that conviction and commitment in the international arena, the INAI regularly participates in the main regional and international cooperation mechanisms, like the GPA, since they are spaces for debate and the generation of knowledge in which international policies and standards are proposed. In these forums, it is possible to position emerging issues on the political-administrative agendas of governments and, at the same time, promote effective dialogue with civil society organizations and other interested actors.

Finally, we would like to make two closing comments.

The first is on the way to the 44th Global Privacy Assembly 2022, which will have the honor of being host by the Personal Data Authority of Turkey under the theme of "A question of balance: privacy in the era of rapid technological advancement," emphasizing the need to balance privacy and technology.

Among the topics that will be addressed are artificial intelligence (AI), ethics and democracy; facial recognition; Emerging technologies; big data; privacy principles, privacy challenges, consumer rights, and many more.

This year 2021, left us with a lesson that the uses and applications of AI can have positive and negative impacts on human rights, depending on how they are developed and used, but above all, with the ethical degree with which such use is governed. As UNESCO says, we need a human-centered artificial intelligence, which must be in the best interest of humanity and not the other way around. It is necessary to "have clear rules" that constrain their behavior and clarify who is responsible for their successes, failures, or mistakes. We need collective reflections regarding its use, and that the principle of ethics and human dignity is continually respected.

Finally, and as a second comment, we would like to thank the members of the GPA for the vote of confidence deposited in the Institute to chair the organization and promote the necessary actions to advance in the fulfillment of the objectives set out in the Strategic Plan 2021-2023. It is an honor for Mexico, through the INAI, to occupy the Presidency of the GPA for 2021-2023, and the Secretariat.

The Strategic Plan for 2021-2023 seeks for the Global Privacy Assembly to:

• To be a highly effective global forum for privacy and data protection authorities.

• To disseminate knowledge, provide practical assistance, and help authorities more effectively perform their mandates.

• To provide leadership at the international level in data protection and privacy.

• To connect and support efforts at a domestic and regional level, in other international forums, and to enable authorities to protect better and promote privacy and data protection.

It has three main objectives:

1. Advancing Global Privacy in an Age of Accelerated Digitalization

– Work towards a global regulatory environment with clear and consistently high data protection standards as digitalization continues at pace.

2. Maximizing the GPA's voice and influence

– Enhance the GPA's role and voice in broader digital policies.

– Strengthen relationships with other international bodies and networks, advancing data protection and privacy issues through observer arrangements.

3. Capacity Building for the GPA and its Members

– Support Members' shared learning from experiences, strategies, and best practices worldwide, including cooperation tools.

All the future work will be coordinated with the current Executive Committee Members that are formed by:

1. The Board of the National Institute for Transparency, Access to Information, and Personal Data Protection of México. Commissioners Blanca Lilia Ibarra Cadena integrates the Board. (INAI'S President), Francisco Javier Acuña Llamas (GPA works coordinator), Josefina Román Vergara (GPA works coordinator), Norma Julieta del Río Venegas and Adrián Alcalá Méndez.

2. Angelene Falk, Information Commissioner at the Office of the Australian Information Commissioner

3. Beatriz de Anchorena, Director at the National Access to Public Information Agency (AAIP), Argentina.

4. Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information, Germany

5. Faruk BĐLĐR, President Commissioner, Personal Data Protection Authority of Turkey (KVKK) (GPA Host 2022).

6. Omar Seghrouchni, President Commissioner, Morocco-National Commission for the Protection of Personal Data Protection (CNDP).

7. Alexander McD White, Privacy Commissioner of the Personal Data Protection Authority of Bermuda.

As Presidency and Secretariat, the INAI will continue to develop clear and high international standards that contemplate the accelerated digitization process to allow the development of cutting-edge technological solutions that benefit society and, simultaneously, guarantee

the protection of personal data and privacy. It will seek to prop up our economies and break down border barriers by supporting electronic commerce to achieve a balance between protecting personal data and taking advantage of technological expansion without creating obstacles to cross-border trade.

We thank each one of you for making this compilation of voices possible to learn from experts on privacy and protecting personal data from a human-centered vision.

INAI Commissioners, Mexico

Chair and Secretariat Global Privacy Assembly

Blanca Lilia Ibarra Cadena

Adrián Alcalá Méndez

Francisco Javier Acuña Llamas

Norma Julieta del Río Venegas

Josefina Román Vergara

Sponsors

Baker McKenzie

Brian Hengesbaugh

Chair of our global data privacy practice

Carlos Vela-Treviño

Head of Technology, Media, and Telecommunications Industry (CIPM)
Baker & McKenzie Abogados, S.C.

A Human-centric Approach to Data Governance

In the current data policy landscape, we often think of the interests of organizations that use data as an asset being pitted against the rights of individuals or data subjects. Under this paradigm, the battle over data is reduced to a zero-sum-game —leveraging data to develop new products or to better engage with customers comes at the expense of privacy rights—; and any assertion of data subject rights impairs a company's ability to be innovative or competitive in the digital marketplace. Effective data governance has the potential to overcome this paradigm, by identifying and promoting areas where the interests of individuals and organizations that collect, process, or transfer personal data —which is to say, virtually any modern business— converge.

For starters, when we speak of "data governance" we're referring to a diverse set of frameworks to help an organization understand how it collects and uses data across its enterprise. By classifying data within an organization and establishing who is accountable for the use of data assets, a robust data governance program ensures that data is reliable and that it is used in ways that are compliant with privacy laws and regulations.

How can human-centric data governance find the elusive common ground between data subject rights and commercial uses of data? On the one hand, the public benefits from strong data governance in a number of ways. By implementing data tracking and defining clear responsibilities for managing data, an organization confirms it can address the invocation of statutory data rights —like the right to access or rectification—promptly and effectively. Moreover, good data governance optimizes data quality and integrity, which in many cases may obviate the need to data subject rights to be asserted in the first place. A data governance policy may also mandate preventative protective measures, like anonymization or aggregation, that serve the privacy-interests of individuals. Most data governance policies will also include provisions on data security, hardening the organization against potential cyber-attacks and preventing personal data within the organization from

being compromised. Accordingly, data subjects can be assured that their data is accurate, secure, and accountable by virtue of data governance.

But it's not just the public that reaps the benefits. Various advantages also pass to the organizations that adopt meaningful data governance programs. We've already seen how data governance mitigates the possibility that personal data will be mishandled or compromised by cyber-attacks. Falling afoul of privacy laws or being the target of a ransomware incident carries significant regulatory, monetary, and reputational risk —and formulating and implementing strong data governance measures is a critical step in managing such risks—. Data governance isn't simply a risk management tool; a well-executed data governance policy can also help an organization to assess its data assets, optimize data flows and identify new ways to leverage data. Additionally, adopting preventative protective measures, mentioned previously, can afford the organization greater flexibility in how it may use the data to support its business interests.

Critically, each of these measures accumulates trust between the organization and its stakeholders. Such trust benefits both the stakeholders and the organization mutually and promotes the sense of common interest. For years, Baker McKenzie has worked with clients to establish data governance structures that enable them to build trusting relationships with their customers and public, navigate an evolving risk landscape, and ultimately become more successful and innovative. Our commitment to human-centric governance principles doesn't end with our work for clients, and we have been privileged to partner with organizations like the Global Privacy Assembly and the World Economic Forum's Centre for the Fourth Industrial Revolution (C4IR) to forge new discussions around emerging areas like the role of legal technology and AI in advancing the protection of privacy.

By adopting a "human-centric" data governance scheme —one that places the interests and expectations of individuals at its core and bridge the interests of organizations that use personal data with the rights of data subjects— both data subjects and data users come out winners.

Clip

Judith Alejandra Nieto Muñoz
Industry Relations Sr Manager Clip

The humans behind the data: perspectives from a Mexican FinTech in the payment's ecosystem.

By now, most of us know that the world has a new favorite "intangible" good: data. What is more, many companies have undertaken a series of deep, costly, and sometimes painful internal restructuring hoping to get on board of this data-driven train apparently destined towards growth. However, we seem to have lost perspective for a moment, and relying too heavily on the power of data and all automated things has proven to be an ineffective way to tackle the challenges that come with the unforeseeable nature of us humans.

Data should be used for the benefit of the many. And we sustain that this is not a naive approach: it is perfectly possible to do business while also advancing a beneficial agenda for society. At Clip, for instance, we have learned that one of the best ways to make our company grow is by being champions for financial inclusion; at the end of the day, the goal is helping our merchants (and their employees and families) improve their lives, while also allowing their consumers the freedom to decide among more payment options.

Therefore, corporations must be transparent not only about which data they collect but also how they may profit from it. We need to acknowledge that the latter has an effect on either closing gaps and solving inequalities or in making them worse. Therefore, we believe that the best path to achieve this considers, at least, the following:

1. Companies must have a clear policy regarding how they manage data (from collection to treatment) and the values that will shape the decisions taken with such data as foundation. Of course, this being open to public scrutiny is vital.

2. Globally, we should be striving for more available, interoperable, and open data. This need not be opposed to personal data protection and privacy, since everyone must conform to the multiple sets of rules and good practices designed specifically for that purpose. Large entities will have very few incentives to evolve their business model and incorporate new perspectives if potential competitors have no access to such valuable information.

3. Regulators need to have both the ability to ensure the rule of law but also to adapt to an ever-changing environment. Working closely with private and public stakeholders (academia, think tanks, NGO's) is necessary if we want to unhinge the power of data and not just have it respond to market interests.

Needless to say, these are merely the basics. While it is crucial to further discuss the intricacies of a human centric approach in data governance, we are convinced that the ultimate goal can unify almost everyone: data is a byproduct of human activity, and it is only fair to put whatever insights we can get from it into advancing towards a more equitable, fair, and inclusive world.

Davara Abogados

Isabel Davara F. de Marcos

Founding Partner and Director at Davara Abogados: a legal boutique specialized in Digital Law, Technology and Innovation.

Mechanisms for active accountability and their role in a human-centered perspective

The protection of personal data has become an increasingly complex and important task for individuals and public or private organizations that process personal data. Data has an undeniable value for organizations and individuals. The legitimate use of data is a legal obligation, but also an ethical duty that has a more far-reaching scope than just regulatory compliance. The protection of personal data is a human right that puts the individual at its center and that is inextricably linked to human dignity and freedom.

Every company or organization must implement a personal data governance system. Setting up the mechanisms that allow the demonstrable and continuous compliance of the obligations set forth in the personal data regulations in force in Mexico, in addition to considering the elements that the current legislation establishes in a clear manner, also implies a broad analysis of whether such measures will continue to be appropriate and functional to guarantee the rights of privacy and personal data protection. In a fast-moving and complex environment in which technology is an essential tool for data processing, the development of a comprehensive and exhaustive compliance program is extremely relevant for organizations to successfully protect this right.

Implementing a personal data compliance program has numerous components, all of them linked to the common objective of guaranteeing the legitimate data processing. The first action that can be considered for this goal is the analysis of the data processes, databases, and applicable legal basis, which will be the raw material for the elaboration of a personal data inventory to document the data flow within the organization. From this point, it will be possible to identify and implement all the subsequent obligations (proportionality, quality, information, etc.).

When identifying the data communications and/or accesses to third parties, it is essential to regulate data transmissions and transfers by using specific clauses, since the participation of third parties in data processing must be strictly regulated. All these actions must be carried by specialized people within the organization in charge of ensuring the compliance of the regulations and the rights of the data subjects. Therefore, organizations must appoint

a Data Protection Officer or Personal Data Department that also serves as a communication and attention channel to the claims of the data subjects.

To comply with the Law, it is crucial that the rights should be addressed systematically and in a timely manner through the creation of records and follow-up schemes. Also, attending to these rights in a diligent and continuous manner will allow to people take free and informed decisions on the use of their data.

The guarantee of the human right to data protection involves the responsibility to implement the appropriate security measures to prevent data from being compromised. The implementation of a security governance scheme guided by a Security Management Policy of Personal Data and the development of detailed security and data protection controls and procedures is essential, as there is no privacy without security.

Finally, we cannot overlook the fact that the implementation of a compliance program of this nature will benefit from specialized counseling, in which law Firms with exclusive dedication to this matter —such as Davara Abogados— are excellent partners for the timely incorporation of active accountability mechanisms.

Deloitte

Data governance in a human centric approach

In a globalized world, and as companies grow and the development of technology accelerates, the processing of personal data and the need to have more and more information becomes greater and indispensable, generating chaos within organizations if the design of data governance is based on a reactive and not a preventive approach. Consequently, the greatest impact falls on the owner of the personal data, who is the most vulnerable.

Under that perspective, having a preventive approach to data governance allows organizations to act under a business ethic based on a risk management methodology, which would benefit data subjects, since it would be defined and approved by senior management and designed and implemented by the different strategic areas of each organization involved in the processing of personal data.

Data governance is made up of a series of guidelines, policies and processes of an organization that ensure that personal data are correct, reliable, useful, and secure. This means that, with proper planning and control, it helps the organization strategically to generate business value from personal data and thus help to achieve its goals, without compromising privacy and respecting the rights and freedoms of data subjects.

To ensure the due exercise of the rights and freedoms of data subjects, it is essential for organizations to have the traceability of personal data, i.e., to know what data they have, how they are collected, where they are stored, with whom they are shared, how they are used and when they should be updated or deleted and how. Hence, the importance for organizations to have a personal data management system, since it allows them to have a comprehensive view of the information, facilitating shared responsibility in decision making.

In addition, data governance should not be static, but should be in constant change, adapting at all times to the needs of the business, new technological developments and new regulations that provide stricter controls and seek to protect privacy with a human-centered approach.

Finally, in Deloitte Spanish Latin America, we are committed to privacy in the processing of personal data of our clients, employees, partners, suppliers and third parties, from its collection, use, disclosure, storage and disposal, applying the necessary controls to comply with the duties, principles and privacy obligations of the applicable laws; for this reason, we have a Personal Data Management System, being the first professional services firm in Mexico with a Binding Self-Regulation certification, which reaffirms our commitment to privacy and protection of personal data, thus confirming the shared values that guide our behavior as professionals and as an organization.

Google

Keith Enright

Chief Privacy Officer at Google

Hello everyone. It was an honor for Google to be a sponsor of the GPA 2021 and we appreciate the opportunity to participate in the first GPA Memory book.

Technology is too often portrayed as a threat to privacy. We find this view to be shortsighted. In fact, technology can unlock the value of information in a way that protects privacy and enhances compliance with local laws.

Expectations of companies are changing: People want better product experiences, better security, and better privacy protections. It is our job to meet or exceed those expectations.

Google applies the same level of investment and innovation to privacy and security protections and regulatory compliance as we do to developing new services, features, and devices. We're guided by three principles:

1. **First**, by keeping your information **secure by default** with advanced, industry leading security: protections are automatically built into your Google Account and into every Google product. Just three examples of this include: Gmail automatically blocking more than 100 million phishing attempts every day; Google Play Protect running security scans on 100 billion installed apps around the world; and to protect people from malicious activity, Google checking 1 billion saved passwords for breaches, daily.

2. **Our second principle is** treating your data responsibly with **privacy by design.** Our key strength is in technological innovation, and we are leaning in hard on developing and deploying the industry's most effective, intuitive, and innovative privacy technologies. We offer data minimization tools like Auto-Delete, which gives you the choice to have Google automatically and continuously delete certain data from your account. We have made Auto-Delete the default setting for all new Google Accounts which means now activity data older than 18 months is automatically deleted for more than 2B users every day. We also invented Federated Learning, a new approach to machine learning that enables processing on mobile devices without centralized training data. And we've built the world's largest open-source library of differential privacy algorithms, helping everyone from cancer researchers to census analysts apply privacy-preserving technology to their work.

3. **Finally**, we provide meaningful controls and tools to users **so they are in control**. Controls should be effective, intuitive, and easy-to-use, which is why we continually improve them. You can find them in your Google Account, which saw over 3 billion visits last year. To maximize user engagement with and understanding of their account settings, we created

a comprehensive Privacy Checkup that helps 500M people a year choose the privacy settings that are right for them. We were the first in the industry to create Takeout to promote data poability, empowering users to easily download their personal data and switch to other services

All around the world, we're focused on constructive and productive engagement with regulators. This is why the GPA is so essential and important every year. Data flows are global, and we need to work with all of you to ensure that strong privacy protections are in place and our products and services can be used with trust and confidence. Clarity and harmonization helps drive compliance, and we welcome the opportunity to share what we're doing and to learn from you all to advance our shared objective of strong compliance.

Thank you again for the opportunity to participate in this GPA Memory Book.

Meta

Technology and data use have changed so much in the past 10 years. I can video chat with relatives worldwide, I never get lost, and I can stay connected to the causes and businesses I care about. As we emerge from the Covid-19 pandemic, technology has helped people find vaccines and get access to authoritative health information.

Changes in technology and data use also raise important questions about how people's privacy is protected. But I am hopeful, because as we create new ways of using data, we can come together as a privacy community to answer hard questions. If we collaborate, we can build technology that empowers people around the world.

Over the past 10 years, Meta's approach to privacy has evolved. What we've learned is that privacy is a fundamental business priority and a real competitive advantage. If people don't trust that we're protecting their privacy, we won't be in business anymore. So, we've continued to improve the way we build privacy into our people-centered products and technology.

For instance, we've been investing in a multi-year effort to build a portfolio of privacy-enhancing technologies, or PETs. These technologies use cryptography and statistical methodologies to minimize how much data we process while preserving people's ability to receive customized services and businesses' ability to ensure their messages get to the right audience. PETs are complex and expensive, but we think they'll be the foundation that powers tomorrow's internet.

Looking ahead, the issues we face around data use are only going to increase in complexity. So much will change in this next decade —especially as we develop the AR and VR technologies of the metaverse—.

The metaverse is not something that Meta is going to build alone. Its success depends on companies developing services that work together and across platforms. In the same way, we will also need to work together to reimagine privacy expectations and protections for this new context.

For example, last year Meta released Ray-Ban Stories, glasses with embedded cameras in the frames that allow you to take short photos and videos. We knew that we needed to consider privacy beyond baseline data protection law and principles. So, we engaged with experts in privacy, civil liberties, and human and civil rights prior to launch.

Because of their feedback, the videos, and pictures you take using Ray-Ban Stories are only sent to Meta servers when you decide to share them. We designed an LED light that would give a clear visual signal when a person uses the glasses to take a picture or record,

and you have to take an obvious action —like pushing a button or saying "take a video" out loud— to take a picture or record a video.

As we innovate in AR/VR, getting privacy right will not be easy. To innovate responsibly, we will continue to seek and implement informed external feedback along the way.

New technologies bring new possibilities —we need to build them responsibly in collaboration with the data protection community—. Getting the future right isn't the purview of one company or one country; privacy is something we all have to protect, together.

Microsoft

Microsoft is a company that has distinguished itself by delivering remarkable innovations that have transformed so many aspects of people's lives for the better.

But we recognize that our success comes with a deep responsibility to be a trustworthy partner to the communities we serve and to governments whose role is to set the parameters of our operations, and the behavior of the tech industry as a whole.

We truly believe, as a principle, in strong privacy and data protection laws that offer control and transparency over how data is being used. We not only respect privacy laws all over the world, but we advocate globally for legal protection of privacy as a fundamental human right.

Governments are moving quickly around the world to create new or modify existing modern data protection laws. By some counts, there are more than120 jurisdictions globally with data protection laws. The question now isn't *if* governments should regulate the collection and use of data, but *how* it should be done.

The European Convention on Human Rights stated in 1950: "Everyone has the right to respect his private and family life, his home and his correspondence". This simple paragraph should be the cornerstone for implementing the how on the processing of personal data.

As data is being regulated more comprehensively, it will be important to think about data in the critical role it plays in our global societies.

It would be helpful to begin with a foundation that embraces the importance of data in building prosperity: the ability to use and share data is what makes breakthroughs that are revolutionizing our lives possible.

Data is essential in helping with the challenges humanity is currently facing like the effort to reduce global carbon emissions and uncover the patterns that affect climate change and impact biodiversity, or for detecting and deterring cyberattacks and keeping our children safe from online predators.

Regulatory frameworks of data governance with a human centric approach should enable us to build a better world, create jobs and opportunities, and protect privacy and other fundamental human rights:

First, the frameworks should encourage —even require— companies to use privacy-enhancing tools that support the responsible use of data by enforcing the data protection principles.

Second, the laws we implement should hold organizations accountable for the harm and abuses that could be caused.

Third, the laws we create must be broad enough to account for both traditional and new business models, especially the ones that use AI for maximizing business opportunities.

Finally, we must focus on the impact of these technologies on people, and craft legislation to empower individuals to control their data and their digital identities.

This is the area where we've seen the most progress through laws like GDPR and the California Consumer Privacy Act that give people ownership of their data by recognizing their right to access, rectify, and delete their own information.

It is crucial to build legal systems that enable data use and governance based on a human centric approach, allowing society to responsibly use and share information to drive innovation, serve the public good, preserve privacy and protect against public and private harms. Our collective goal should be to create aa balance that enables society to benefit, people to feel safe, and economies to thrive.

NYCE MX

The protection of personal data is a right that has become relevant recently, in particular with the advent of social networks and the advancement of technology that allow to give traceability to the habits of users, storage, and processing of large amounts of information with low-cost equipment, the processing with artificial intelligence applications, machine learning and Big Data, as well as the ease with which users have adopted these technologies. In this way the new business models are no longer always based on payment for Services in a current currency, now many applications and Services provide their access and use in exchange for the user allowing their personal data to be collected and sometimes that of their contacts or acquaintances.

Therefore, we must see the protection of personal data as a matter beyond protecting data, because it is about protecting the individual rights and guarantees of the person, who must be the center of the treatment and who decides on who is provided with their data and what is done with them.

Mexico was one of the first countries with a personal data regulation according to the new models, even before other regions such as Europe with GDPR, allowed the generation of lessons learned, as well as the adoption and establishment of good practices that positioned Mexico as an important reference at the international level. In fact, the ISO/IEC 27701 standard, which is focused on establishing controls that extend the scope of an Information Security Management System to consider the protection of personal data and the privacy of the principals, had references in the Mexican model and has become a success story both regionally and internationally, so that today, through certification in this standard, compliance with self-regulation schemes can be demonstrated and in turn with the principles of duties and obligations contained in the Law, its Regulations and other secondary regulations in the matter, but this also allows compliance with the obligations established in other regulations, for example, the one applicable in the European Union through GDPR.

The practices contained in these management models for the protection of personal data include practices such as:

– Carry out an inventory of personal data that allows to give traceability to the treatment of the data through the data processing systems and the people who carry it out throughout its life cycle

– Establish roles, functions and responsibilities of personnel and subcontracted organizations with respect to the processing of personal data

– The allocation of economic, material, human, as well as organizational resources to carry out the actions defined by the management system

– Perform a risk analysis on events and consequences that may lead to compromising personal data

– Carry out a Privacy Impact Assessment that identifies the purpose and proportionality of the processing of personal data, justifying its treatment and minimizing its collection as well as its retention period

– Determine administrative, physical, and technical security measures to address the risks identified in the privacy impact assessment and risk analysis

– Carry out reviews and audits to identify possible deviations in the implementation of the defined actions

– Maintain and continuously improve the management system, implement corrective and improvement actions as appropriate

All these actions must be considered in constant review and update, since the advances in the relationship, technology, as well as in the threats and agents that can carry out a breach are constantly changing and evolving.

Currently the use of face recognition tools and other biometric data allow to identify a person with a very high level of certainty, this has laudable uses for the control of access to buildings, identification of criminals, provision of health services, etc. But they can also be used as repressive measures, segmentation, discrimination, and coercion of human rights. In this way, a balance must be maintained between the benefits of the use of technologies, with the possible consequences that a breach may have on the impact on privacy and the rights of the principals. For this, the implementation of controls such as the dissociation, segmentation and data encryption, as well as the authentication of people and devices, the authorization of the actions to be executed according to the roles permissions and privileges that they must have according to their functions, and the constant monitoring of the processing of the data to identify, protecting, contain, respond to and recover from incidents are basic actions that every organization must implement.

Twitter

Damien Kieran
Twitter Chief Privacy Officer

Renato Leite Monteiro
Twitter International Privacy and Data Protection Lead

Depending on where you are in the world, each of us has experienced the impact of the pandemic in different ways. And technology had a deep role in the way we experienced the pandemic.

However, technology is an instrument, a tool. Like many tools it can be used for good and not so good things. Perhaps a way to think about it, is that technology in its rawest form is an exceptionally powerful tool. As a result, depending on how that tool is used it can be a vector for both creating more or less trust: Create bridges and break bridges, empower, and disempower, educate, and misinform, and so on.

But for sure technology can help serve the public good. For many citizens of the world, the pandemic was a time where they used technology to "live". It enabled them in good ways. To enable "living", over the last two years we arguably accelerated global usage of data driven technologies. Data was harnessed to help with vaccines, shopping, working from home, re-establishing travel and so many other things. But with those benefits also came a broader recognition of the challenges and concerns around how data is used, like no other time in history.

Whether it's access to technology that results in social exclusion and the de facto denial of civil rights and freedoms or technology itself and the inherent risks of poorly considered and executed technology. To offset these challenges, organizations, together with governments, need to guarantee the most basic fundamental rights, among them, privacy.

Therefore, we need to be thoughtful and deliberate in building technologies and structures that reward the design and development of rights respectful products and services. That is why it is critical to create strong foundations that enable technology to be used for building trust, through appropriate regulation, accountability, education, data standardization, engineering guardrails and much more.

Unfortunately, an increasing patchwork of regulations continues to develop around the world. This will have significant impacts on how data driven technologies operate and how they may differ from country to country or region to region with possibly negative outcomes

for people. So, while technology "can" live up to expectation, we also have to enable it to live up to expectations.

At Twitter, building respectful products and services that enable the public conversation is what we strive to do. We work each day to build practices and technologies that deliver on that objective. For that, we need to respect people's privacy.

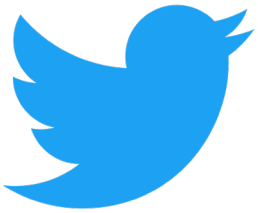
At Twitter, "privacy is a fundamental right that everyone who uses our services has, and we need to be clear in terms of what those rights entail —serving them first and us second—". But that's not a new thing for Twitter. Privacy and protecting the people that use our services has been part of our identity since Twitter was launched. Nonetheless, in times of pandemic, in special, these commitments are crucial.

For example, during the pandemic, we have worked diligently to enable healthy conversations, including around COVID. This saw us launch our COVID misleading information policy and take actions to ensure the information people were seeing around COVID was accurate. For this we obviously needed to harness data for good, while respecting people's privacy.

The point is these are things we care deeply about. Our overarching goal is to protect people and increase their trust in our platform so we can continue serving the public conversation —including by ensuring it's healthy—. That's why the internal motto that drives our data stewards' program is: "Trust is earned not given".

We couldn't have done it without you! Thank you!


salesforce




Meta


Google


Microsoft


aws


Baker
McKenzie.


Deloitte.


NYCE
A QIMA COMPANY


DAVARA
ABOGADOS


clip

Global Privacy Assembly Members and Observers

Members


KOMISIONERI PËR TË DREJTËN
E INFORMIMIT DHE MBROJTJEN
E TË DHËNAVE PERSONALE


Office of the Information Commissioner
Queensland


apda
Agència Andorrana
de Protecció de dades


Information
Commissioner
NORTHERN TERRITORY


OVIC


Agencia de Acceso
a la Información Pública


Република България
Комисия за защита на личните данни


MINISTRY OF JUSTICE OF THE REPUBLIC OF
ARMENIA


OAIC


ipc
information
and privacy
commission
new south wales


oipc
OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA


dsb
Republik Österreich
Datenschutz
behörde


Manitoba
Ombudsman
Ombudsman ■ Information Access and Privacy ■ Whistleblower


Gegevensbeschermingsautoriteit


OIPC


CNIL


OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
NORTHWEST TERRITORIES


Personal Data Protection Agency
in Bosnia and Herzegovina


Privacy Commissioner
Bermuda | Quo Data Ferunt

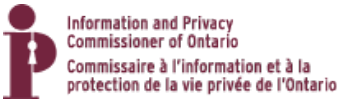

DATATILSYNET


Office of the Information
& Privacy Commissioner
Nova Scotia
OIPC


EDPS

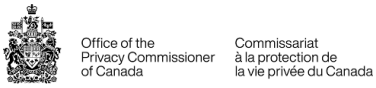

OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
OF NUNAVUT


Republic of Estonia
Data Protection Inspectorate


Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario


Commission
d'accès à l'information
du Québec


CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS


Office of the
Privacy Commissioner
of Canada
Commissariat
à la protection de
la vie privée du Canada


CNPDCP


ARTCI


STATE
INSPECTOR'S
SERVICE

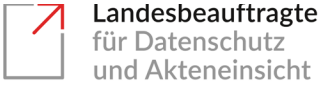

Office of the Commissioner for Personal Data Protection
Independent Supervisory Authority for the protection of the individual

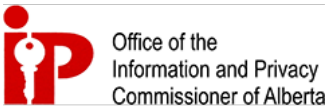

Commission de l'Informatique
et des Libertés – Burkina Faso


COUNCIL OF EUROPE
CONSEIL DE L'EUROPE


Berliner Beauftragte
für Datenschutz
und Informationsfreiheit


Industria y
Comercio
SUPERINTENDENCIA

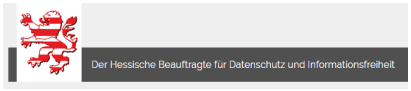

Landesbeauftragte
für Datenschutz
und Akteneinsicht


Office of the
Information and Privacy
Commissioner of Alberta


úřad pro ochranu
osobních údajů
the office for personal
data protection


New Nouveau
Brunswick
CANADA


Office of the
Saskatchewan Information
and Privacy Commissioner


Der Hessische Beauftragte für Datenschutz und Informationsfreiheit


Der Landesbeauftragte für Datenschutz
und Informationsfreiheit Mecklenburg-Vorpommern


Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz


sachsen.de


ULD


BfDI
Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit


CNPD
Comissão Nacional de Protecção de Dados


DPC
DATA PROTECTION
COMMISSION


ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ
ΔΕΔΟΜΕΝΩΝ


Nemzeti
Adatvédelmi és
Információszabadság
Hatóság


GRA
GIBRALTAR REGULATORY
AUTHORITY


OMBUDSMAN
CAYMAN ISLANDS


PCPD
私隱公署


PERSÓNU
VERND


inai


info


An Coimisiún um
Chosaint Sonraí
Data Protection
Commission


information
commissioner
Barrantagh Fysseree


GPDP
25
1997-2022


JOIC
JERSEY OFFICE OF THE
INFORMATION COMMISSIONER


consejo para la
Transparencia


CIISD
Canadian and International
Industrial Security Directorate

개인정보보호위원회

REPUBLIC OF KOSOVO
NATIONAL AGENCY FOR PROTECTION OF PERSONAL DATA

Datu valsts inspekcija

DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

State Data Protection Inspectorate

azop Croatian Personal Data Protection Agency

Dubai International Financial Centre

CNPD
Commission nationale pour la protection des données
Grand-Duché de Luxembourg

ДЗЛП

Freie Hansestadt Bremen

APDP

idpc. INFORMATION AND DATA PROTECTION COMMISSIONER

Niedersachsen

DPO
Data Protection Office

National Center for Personal Data Protection of the Republic of Moldova

CNDP

AUTORITEIT PERSOONSGEGEVENS

Privacy Commissioner
Te Mana Matapono Matatapu

Datatilsynet
The Norwegian Data Protection Authority

NATIONAL PRIVACY COMMISSION

GIODO Zapraszamy na nową stronę internetową Urzędu www.uodo.gov.pl Urząd Ochrony Danych Osobowych

CNPD

Autorità Garante per la Protezione dei Dati Personali

LDI NRW

SACHSEN-ANHALT
Landesbeauftragter für den Datenschutz

TLfDI
Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit


ÚRAD NA OCHRANU
OSOBNÝCH ÚDAJOV
SLOVENSKEJ REPUBLIKY


INFORMACIJSKI
POOBLAŠČENEC


Bayerisches Landesamt für
Datenschutzaufsicht


Generalitat
de Catalunya

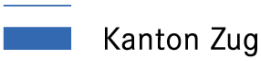

Hamburg
Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit


aepd
agencia
española
protección
datos


THE OFFICE OF THE
Data Protection
Authority


IMY.


CCF - INTERPOL


Kanton Zug


הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية


Datenschutzbeauftragter des Kantons Basel-Stadt

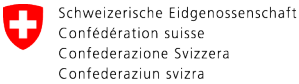

個人情報保護委員会
Personal Information Protection Commission


dsb
datenschutzbeauftragte
des kantons zürich


KISA
Korea Internet & Security Agency

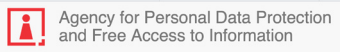

BASEL
LANDSCHAFT


Republic of North Macedonia
Personal Data Protection Agency


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra


CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES


INPDP


Agency for Personal Data Protection
and Free Access to Information


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU


Privacy Commissioner
Office of the Privacy Commissioner


OECD
BETTER POLICIES FOR BETTER LIVES


ico.


PERÚ
Ministerio de Justicia
y Derechos Humanos


ANPDP
Agência Nacional de Protecção de Dados Pessoais


Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos


CDP
Commission de Protection des Données Personnelles


Kanton Bern
Canton de Berne


REPUBLIC OF SLOVENIA
HUMAN RIGHTS OMBUDSMAN


Ukrainian Parliament
Commissioner
for Human Rights


INFORMATION
REGULATOR
(SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information


PRODHAB
AGENCIA DE PROTECCIÓN DE DATOS DE LOS HABITANTES
MINISTERIO DE JUSTICIA Y PAZ

Observers

CICR

Canadian International Industrial
Security Directorate

IFRC

مركز قطر للمال
Qatar Financial Centre

IIDH
INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
INSTITUT INTERAMÉRICAIN DES DROITS DE L'HOMME
INSTITUTO INTERAMERICANO DE DIREITOS HUMANOS
INTER-AMERICAN INSTITUTE OF HUMAN RIGHTS

وزارة المواصلات
MINISTRY OF TRANSPORT

IOM UN MIGRATION | MAKING MIGRATION WORK FOR ALL

SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

THE UNITED STATES DEPARTMENT of JUSTICE

United Nations | Secretary-General

中華人民共和國澳門特別行政區政府入口網站
Government Portal of Macao Special Administrative Region of the People's Republic of China

UNHCR
The UN Refugee Agency

MyGovernment
The Government of Malaysia's Official Gateway

NETWORK OF AFRICAN DATA PROTECTION AUTHORITIES
REDE AFRICANA DAS AUTORIDADES DE PROTECÇÃO DE DADOS PESSOAIS
RÉSEAU AFRICAIN DES AUTORITÉS DE PROTECTION DES DONNÉES PERSONNELLES

Homeland Security

OECD
BETTER POLICIES FOR BETTER LIVES

U.S. DEPARTMENT OF COMMERCE
NTIA
NATIONAL TELECOMMUNICATIONS & INFORMATION ADMINISTRATION

U.S. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Photo gallery


GPA
Global Privacy Assembly
inai


#GPA2021
inai


inai
GPA
Global Privacy Assembly

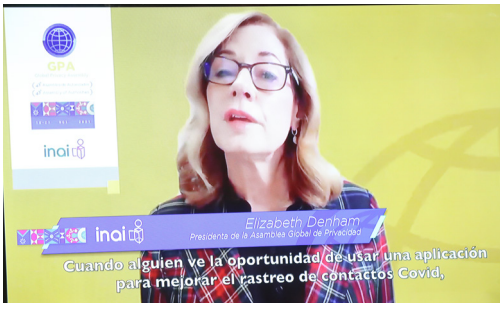

inai
GPA
Global Privacy Assembly


FUNCIÓN PÚBLICA
SECRETARÍA DE LA FUNCIÓN PÚBLICA


OCDE
OECD
Colegas, gracias por la oportunidad de hablarles hoy en un momento crítico para la privacidad y la protección de datos.


GPA


inai
Enrique Graue Wiechers
Rector de la Universidad Nacional Autónoma de México


GPA
inai
inai
Elizabeth Denham
Presidenta de la Asamblea Global de Privacidad
Cuando alguien ve la oportunidad de usar una aplicación
para mejorar el rastreo de contactos Covid,