ISSUE 3
SEP, 2022

NEWSLETTER

GPA
Global Privacy Assembly

p. 03

'WHAT'S GENDER GOT TO DO WITH PRIVACY AND DATA PROTECTION?"

HORIZON SCANNING (ELIZABETH COOMBS)

Do we protect those whose enjoyment of privacy and data protection rights are affected by their gender? Research on women's and transgender individuals' experiences of the right to privacy reveals these differ from cisgender straight males'. The absence of gender data in privacy and data protection reporting and policy development suggests an opportunity for the GPA and its aim of international regulatory and policy leadership.

p. 12

"PROTECTING AGAINST GENDER-BASED PRIVACY HARMS"

IN CONVERSATION WITH COMMISSIONER ANGELENE FALK

Protecting against gender-based privacy harm requires implementing privacy protections that consider gender implications.

p. 14

OBSERVER ON THE ROAD

JOSÉ LUIS MICHELENA ICRC

Each time an individual is referred to a humanitarian organization personal information becomes vulnerable to a host of data and privacy-related risks. Protecting this data is a vital ethical obligation to which all humanitarian actors are bound.

INDEX

MESSAGE FROM THE CHAIR





In a world where an entire generation has been raised in the digital era and where the COVID-19 pandemic sped the digitalization of our work, school, home, and social spaces; and whilst this digitalization created opportunities for many, it also underscored the existing digital and gender gaps, and gave rise to new expressions of gender-based violence.

At the same time, with the advent of artificial intelligence, there are several considerations to be made in terms of the gender imbalances it presents. On the one hand, gender disparity in science is one of the most focused debating points among authorities and the scientific community, where women still represent a minority in the fields of technology development[1], and on the other; gender biases risk further stigmatizing and marginalizing women and gender-diverse people putting them at risk of being left behind in all realms of economic, political, and social life.

According to UNESCO's 2019 report ***"I'd Blush if I Could"***, closing gender divides in digital skills through education, unambiguously shows that the gender biases found in AI training data sets, algorithms and devices have the potential of spreading and reinforcing harmful gender stereotypes[2].

This digitalization and the proliferation of artificial intelligence systems have brought about a range of risks for vulnerable populations such as women and, sexually and gender-diverse people (transgender, queer, non-binary, asexual,

1 https://www.unesco.org/reports/science/2021/en

2 https://unesdoc.unesco.org/ark:/48223/pf0000374174

intersexual) face unique experiences and challenges when it comes to privacy and data protection[3]. Data treatment and privacy laws without a gender perspective increase the vulnerability of these already vulnerable groups and pose serious risks to their physical integrity, employment opportunities, financial security, access to healthcare, and many more.

There are several international agreements that explicitly reference gender perspective and the right to privacy and data protection such as the United Nations' Universal Declaration on Human Rights; the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) which in its 65th article states that:

"Data Protection Personal data shall be stored and used pursuant to the obligations undertaken by the Parties under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)."[4]

In April 2016, the EU adopted a new legal framework - the General Data Protection Regulation (GDPR) and the Data Protection Directive for the law enforcement and police area. Fully applicable across the EU in May 2018, the GDPR is the most comprehensive and progressive piece of data protection legislation in the world, updated to deal with the implications of the digital age.

In 2021, the Organization of American States (OAS) unanimously approved the "Updated Principles on Privacy and the Personal Data Protection". This process incorporated for the first time ever a cross-cutting gender and human rights perspective stating that *"the Principles are interrelated and should be interpreted together as a whole, with a cross-cutting gender and human rights perspective that identifies the differentiated impacts of Data Processing and makes them visible to allow for Data Controllers and Processors to take the necessary measures to mitigate these disparities and prevent said Processing from undermining the dignity and privacy of persons facing situations of particular vulnerability"*[5].

While the GDPR[6] recognises data related to sex life and sexual orientation as special categories. Other models, such as SADC (South African Development Community) recognise gender as sensitive data[7]. However, most legislation on data protection does not recognize gender as a sensitive category.

When we fail to recognize women and girls, sexually and gender diverse populations as vulnerable populations[8] and therefore as sensitive categories we jeopardize these populations. However, if we consider the potential harms associated with the collection of gender sensitive data can help ensure these are mitigated (such as gender-based violence and discrimination).

While the legal frameworks exist, gender has been notably absent from the data and privacy protection conversation. As data and privacy protection authorities we must consider the intersection between data, technology, and gender. It is our responsibility to have these conversations and move towards the implementation of a gender perspective in all mechanisms, programmes and policies we develop to guarantee the human right to privacy.

3 https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf

4 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

5 https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf

6 https://gdpr-info.eu/

7 https://www.sadc.int/

8 https://www.un.org/en/fight-racism/vulnerable-groups

‘WHAT’S GENDER GOT TO DO WITH PRIVACY AND DATA PROTECTION?’

Elizabeth Coombs, GPA Reference Panel Member Immediate Past Privacy Commissioner New South Wales, Australia.

‘What do we protect when we protect privacy and ensure data protection?’ asks a GPA Working Group paper.[1] The corollary, ‘what don’t we protect when we protect privacy and ensure data protection?’ is worth asking also. One answer clearly is in the title, that is, those whose enjoyment of privacy and data protection rights are affected by their gender.

First though, some terminology: ‘gender’ and ‘sex’ are frequently used interchangeably, although sex, sex life, sexual orientation and sex characteristics have different, while related meanings. And ‘gender’ can be misunderstood to refer only to females. Glossaries explain gender terms more comprehensively than possible here, but, in short, ‘gender’ is meant as a psychological, cultural and social construct, and an important part of personal identity. People identify their gender as masculine, feminine, transgender, other or none (indeterminate/ unspecified).[2] The United States, like Australia, New Zealand amongst others, has introduced passports with an X, or ‘non-binary gender marker’.

International human rights jurisprudence has established the right to privacy concerns sexual orientation and gender identity[3] and recognised that losses of privacy or protection of information about one’s gender can have significant adverse consequences. Further, lack of autonomy, economic

1 PSWG3: ‘Privacy and data protection as fundamental rights: A Narrative’ prepared for the GPA WG3 on Privacy and Human Rights, 2021, https://globalprivacyassembly.org/wp-content/uploads/2022/03/PSWG3-Privacy-and-data-protection-as-fundamental-rights-A-narrative-ENGLISH.pdf

2 Council of Europe, 2022 Gender Matters: Glossary https://www.coe.int/en/web/gender-matters/glossary; Council of Europe, 2022, Gender Matters, https://www.coe.int/en/web/gender-matters/exploring-gender-and-gender-identity.

3 Communication No. 2172/2012 2 December 2011; 17 March 2017, CCPR/C119/D/2172/2012, par. 7.2.

harm, damaged reputations, and violence can produce severe physical and mental health impacts.[4] Infringements arise across a wide variety of circumstances - migration, adoption, identity systems, banking, dating apps, education, housing – the list goes on and continues to grow as digital technologies, such as AI, apply more widely, and as gender information is increasingly monitored and monetised.

Research on women's and transgender individuals' experiences of the right to privacy reveals these differ from cisgender straight males'. Women for example, are less likely than men to exchange certain types of sensitive information and unique identifiers, and to have less control over their data.[5] Discrimination based on gender identity or sex characteristics arising from privacy infringements and failure of data protection is a disproportionate reality for women, intersex and gender diverse individuals, and is frequently compounded by race, socio-economic status and other factors.[6]

While the range of situations and harms are extensive, regulatory safeguards are not. And are perceived as such.[7] This trust deficit undermines societies. Democracy is also undermined when privacy violations restrict other rights such as health, freedom of opinion, of association, of religion and of expression.

THE GENDER GAP IN PRIVACY, DATA PROTECTION AND DIGITAL TECHNOLOGIES

Although the rights to data protection and privacy are experienced differently by gender,[8] data protection law in its many forms around the world, rarely, if at all, addresses 'gender' or 'gender identity'. Sex, sex life or sexual orientation even if included as 'protected information' or 'special categories of data' or 'sensitive information' do not necessa-

ELIZABETH COOMBS

GPA Reference Panel Member and Immediate Past Privacy Commissioner New South Wales, Australia.

4 Annex 2: The Human Right to Privacy: A Gender Perspective:'Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics', Consultation Report of UNSRP Thematic Taskforce 'Privacy and Personality'; Sahebi, S. and Formosa, P., (2022) Social Media and its Negative Impacts on Autonomy, Philosophy and Technology, 35:70, https://doi.org/10.1007/s13347-022-00567-7.

5 Sórum, H., Eg, R and Presthus, W., A Gender Perspective on GDPR and Information Privacy. Procedia Computer Science 196 (2022) 175-182; OAIC (2020) 'Australian Community Attitudes to Privacy Survey 2020'. https://www.oaic.gov.au/__data/assets/pdf_file/0015/2373/australian-community-attitudes-to-privacy-survey-2020.pdf

6 'Research: A Feminist Approach to the Right to privacy and Data Protection', Mozilla, December 8, 2020; https://foundation.mozilla.org/en/blog/research-feminist-approach-right-privacy-and-data-protection/

7 UNSRP Thematic Taskforce opcit. https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf; Theilen, J.T., Baur, A., Bieker, F., Ammicht Quinn, R., Hansen, M. and González Fuster, G. (2021) Feminist data protection: an introduction. Internet Policy Review, 10(4). https://doi.org/10.14763/2021.4.1609

8 SRP Thematic Taskforce 'Privacy and Personality' ibid.

rily provide protection for gender harms.[9] Even the General Data Protection Regulation does not fully engaged with gender as a possible category of harm, although information on sex life and sexual orientation is a 'special category of personal data'.[10]

Privacy and data protection regulation blind to gender and gender harms is ill-equipped to address the differential and biased effect of digital technologies, like AI, upon women and gender diverse individuals.[11]

When technologies such as AI can be gender biased and discriminatory, it´s time to ensure privacy and data protection address the sensitivities and harms associated with an individual's gender, including for intersex, transgender and diverse individuals. While working within their legislation, privacy and data protection authorities (P&DPAs) can help achieve gender equity in privacy rights by improving the visibility of these issues, amongst other actions.[12]

'WHAT GETS MEASURED, GETS DONE'

The 'gender data gap' concerning lesbian, gay, bisexual, transgender and intersex (LGBTI) individuals is a priority for the UN, the European Commission and other regional entities.[13] P&DPAs gather considerable data, including trends over time on total numbers of complaints, data breach statistics, and use of various enforcement and sanction actions. Notwithstanding this, the quantum and nature of interactions of women and gender diverse individuals with data protection regulation is difficult to find. P&DPAs' annual reports do not routinely report complaints and data breach statistics disaggregated by sex or gender[14] - although the metric is seen as relevant to staffing,[15] and in privacy awareness surveys.[16] Recognition, however, of the needs for a gender focus in privacy and data protection is evidenced by public reporting of investigations involving gender issues such as 'outing' of asylum seekers,[17] staff and community training,[18] and privacy guidance for legislative drafting,[19] and LGBTIQ+ communities.[20]

In 2013 the OECD noted the evidence base available for policymaking in privacy was uneven and privacy enforcement authorities' complaint data, breach statistics and other indicators were a potentially rich source of insights for policy makers.[21] The ICDPPC (now GPA) committed to "closing the gaps" and assisting the development of internationally comparable data protection and privacy metrics. However, ICDPPC

9 European network of legal experts in gender equality and non-discrimination (2018) 'Trans and intersex equality rights in Europe: Comparative analysis', van den Brink, M. and Dunne, P. https://ec.europa.eu/info/sites/default/files/trans_and_intersex_equality_rights.pdf

10 Chair, C. (2020) 'My Data Rights: Feminist Reading of the Right to Privacy and Data Protection in the Age of AI', https://mydatarights.africa/wp-content/uploads/2020/12/mydatarights_policy-paper-2020.pdf

11 Coombs, E. and Abraha, H. 'Governance of AI and Gender: Building on International Human Rights Law and relevant regional frameworks', accepted for publication in 'Handbook on the Politics and Governance of Big Data and Artificial Intelligence' Elgar Handbooks in Political Science, editors: A. Zwitter & O.J. Gstrein, 2023.

12 UN Special Rapporteur on the Right to Privacy, GPA Newsletter 2020/21 Vol 2, No. 2.

13 European Commission, List of actions by the Commission to advance LGBTI equality https://ec.europa.eu/info/sites/default/files/lgbti-actionlist-dg-just_en.pdf; UNDP, World Bank Propose Indicators to Measure LGBTI Inclusion in Development, March 2019, https://sdg.iisd.org/news/undp-world-bank-propose-indicators-to-measure-lgbti-inclusion-in-development/; Bell, M. (2017) Analysis and comparative review of equality data collection practices in the European Union Data collection in relation to LGBTI People, European Commission, Directorate-General for Justice and Consumers, https://ec.europa.eu/info/sites/default/files/report_data_collection_in_relation_to_lgbti_people_.pdf

14 Coombs, E. and McKee, K., 'The 'missing women' in data protection reporting'. Reviewed in 2018 and 2022 (English only) members' most recent annual reports. https://iapp.org/news/a/the-missing-women-in-data-protection-reporting/

15 Eg annual reports of Albania, Czech Republic, Moldova, Federal DPIC Switzerland, OAIC, ICO.

16 OAIC (2020) Opcit.

17 Federal Data Protection and Information Commissioner, Germany Activity Report 2021 https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Taetigkeitsberichte/30TB_21.pdf?__blob=publicationFile&v=3

18 Eg Bermuda (2022) https://www.privacy.bm/blog; ICO Information Commissioner's Annual Report and Financial Statements 2021-22, July 2022, HC 392 https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf

19 Eg Commissioner for Information of Public Importance and Personal Data Protection Serbia 2021 Annual Report, https://www.poverenik.rs/en/o-nama/annual-reports.html

20 Eg Commissioner Privacy and Data Protection, Victoria Australia, https://ovic.vic.gov.au/about-us/documents-and-publications-we-produce/annual-reports/

21 OECD (2013) 'Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

Resolutions for Developing New Metrics of Data Protection Regulation (2016) and Big Data (2014) make no mention of gender (or sex) metrics.

While there has been growing awareness of 'gender' in social, legal, educational, technological, media and economic spheres, it has not been raised as an issue for data protection attention in the ICDPPC/GPA's Strategic Directions (2019-21; 2021-2023), Statements, Communiques and Declarations.[22] Although the ICDPPC/GPA has adopted resolutions for specific groups, such as Children's Online Privacy Protection Act (2008) and Human Rights Defenders at Risk (2016), and referred to particular demographic groups such as children and students within generic subjects, for example, the 2021 'Resolution on Data Sharing for the Public Good'.[23]

Policy questions flow from knowing women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics experience privacy differently. Analyses of preliminary questions such as 'Who complains to P&DPAs? For what reason? And with what success?' and 'Are privacy matters involving gender aspects more difficult to resolve?', may be undertaken within P&DPAs but available documentation does not quantitatively or systematically report privacy experiences from gender perspective. A more comprehensive and nuanced evidence base for public policy development, legislative reform, resource allocation and service delivery would be available if analysis by gender or just female/male, was available.

Circling back to the starting point, the absence of gender data in privacy and data protection reporting and policy development suggests an opportunity for the GPA and its aim of international regulatory and policy leadership,[24] to better protect and promote privacy and data protection for all.

22 https://globalprivacyassembly.org/document-archive/

23 43rd Closed Session of the Global Privacy Assembly October 2021.

24 GPA 'Strategic Directions 2021-2023', p6.

IN CONVERSATION WITH

PRIVACY DATA PROTECTION AND GENDER-SENSITIVE ISSUES IN GEORGIA

Prof. Dr. Lela Janashvili
Head of Personal Data Protection Service of Georgia

The fundamental right to personal data protection has gained distinguished prominence in the European legal framework[1] and the autonomy from the right to privacy[2]. The convergence of the right to privacy and personal data protection has transformed. The right to privacy covers issues concerning personal data processing, yet its scope and meaning go far beyond the data privacy law.[3] It embraces issues related to the physical and moral integrity of individuals, gender identification, etc.[4] Nowadays, data-driven decision-making may also lead to hidden discrimination on the grounds of age, sex, etc.[5] Personal Data Protection Service of Georgia aims to integrate a gender perspective through privacy right and strives for better data protection for all individuals.

In Georgia, personal data protection is regulated by an overarching legislative act. Georgian Law on Personal Data Protection regulates the processing of personal data by private and public

1 Van Den Heuvel K., Van Hoboken J., The Justiciability of Data Privacy Issues in Europe and the US, in: Research Handbook on Privacy and Data Protection Law, Fuster G. G., Brakel R. V., Hert P. D. (eds.), 2022, 78.

2 De Terwangne C., Privacy and Data Protection in Europe: Council of Europe's Convention 108+ and Europe Union's GDPR, in: Ibid, 12.

3 Ibid, 76.

4 See, Harris D. J., et al., Law of the European Convention on Human Rights, 3rd ed., 2014, 536-589, in: Ibid, ft. 17.

5 Vrabec H. U., Data Subject Right under the GDPR, with a Commentary through the Lens of the Data-driven Economy, 2021, 8.

institutions, including law enforcement agencies. The Georgian model of data protection legislation is similar to the European one, where the domestic and international regulations envisage the functioning of the law applicable to all sectors under the so-called "umbrella" legislation. Since the adoption of the Georgian Law on Personal Data Protection, several amendments have been introduced to ensure harmonization with European data protection standards. The Personal Data Protection Service actively works on the new draft law for ensuring further compliance with the internationally recognized standards in the field of privacy and personal data protection.

Although the current legislation and policy documents establish various mechanisms for gender equality, still gender-sensitive data processing is a pressing issue. Data concerning an individual's sex life or sexual orientation includes data on the exact identity of an individual's partner(s), thus is perceived as sensitive data, processing of which entails relevant risks.[6] Georgian Law recognizes data related to sex life as a special category, which falls under the specific regulatory regime. Data processing in the digital age itself still increases the risks of illegal processing of relevant databases, illegal surveillance, and other violations. Thus, gender-related data is significantly sensitive and must be treated with extra diligence while processing.

Considering the mentioned challenges, the Personal Data Protection Service acknowledges the role the right to privacy plays for women and gender-diverse individuals. Based on the analysis of high-risk areas for data processing, an annual plan of inspections is being developed in the framework of which the public and private institutions are systematically examined. The Service's equality-oriented approach to gender-sensitive issues is well-demonstrated by the fact that the target group of 'women' and their data protection are defined as one of the priority categories via the Scheduled Examinations (Inspections) Plan of the Service, this year[7]. Accordingly, the scheduled inspections will be conducted based on the target groups which encompass women, migrants and juveniles, also, based on relevant fields, which include labor relationships, covert investigative actions, electronic communications, and modern technologies. The scheduled inspection will be conducted in a maternity hospital for inspecting the legality of data processing of data subjects giving birth.

PROF. DR. LELA JANASHVILI

Head of Personal Data Protection Service of Georgia

Order - 04 of March 2, 2022, of the Head of the Service "On the Approval of the Rules for Studying the Legality of Personal Data Processing", authorizes to conduct a full-scale inspection, request any document/information, enter the premises of the institution, and obtain evidence. Moreover, the Service periodically holds meetings, public lectures for various stakeholders, and issues relevant recommendations and guidelines.

The Personal Data Protection Service will summarize the outcomes and general observations of the conducted activities in its annual report, which will be publicly available via the official webpage.

6 Voigt P., Von Dem Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 110-111.

7 Order - 01/23 of April 7, 2022, of the Head of Personal Data Protection Service "On the Approval of the Scheduled Examinations (Inspections) Plan for the 2022 year". The Inspections Plan is publicly available via the official webpage of Personal Data Protection Service, <www. personaldata.ge>.

IN CONVERSATION WITH

IS ARTIFICIAL INTELLIGENCE (AI) GENDER-NEUTRAL?

Jong In Yoon
Chairperson of Personal Information Protection Commission of Korea (PIPC)

ARE SCIENTIFIC TECHNOLOGIES GENDER-NEUTRAL?

One might believe so as such technologies in modern times rely on logical and sophisticated methodologies agreed upon by experts. An uncomfortable fact has however come to the fore that many scientific studies have affected males and females differently, including in the case of one research that shows vehicles designed for men are less safe for women. The research showed that an airbag designed to fit men might hurt women or children more severely, or even kill them who are relatively shorter when seated and susceptible to shock while it expands under strong pressure.

This tendency continues in the age of the Fourth Industrial Revolution represented by Big Data. The various kinds of data accumulated so far by mankind contain not only social, economic and cul-

tural bias and discrimination but gender aspects while it is scientifically proven that the knowledge created through such research and development can also be gender-biased.

A wide range of convergent technologies in ICT such as algorithms and AI based on the analysis and use of such data have led to the infringement of fundamental human rights including privacy violations and sexual discrimination.

The Personal Information Protection Commission (PIPC) of Korea has taken enforcement action on two AI-related cases since its restructuring as an independent supervisory authority in August 2020. In one case, the PIPC imposed an administrative fine on the Ministry of Justice for feeding the personal information of Korean citizens and foreign nationals into machine learning algorithms in the process of developing an AI-based tracking system in its effort to beef up border control since 2019.

In the other case the PIPC sanctioned an AI technology company and developer of a chatbot called "Iruda" for its violation of the Personal Information Protection Act (PIPA). This is the first case where the PIPC in its official capacity as the regulator of Korea has investigated and taken enforcement action against breaches of the PIPA involving AI machine learning and service datasets, which is significant in that it would provide guidance on personal information processing when it comes to developing and using AI technologies.

Aside from AI-related violations of the PIPA, this case brought up controversy over the illegality of AI use in Korea. The chatbot "Iruda" designed to mimic the language patterns of a 20-year-old female college student became popular among teenage users in particular. Some male users would however sexually objectify "Iruda," in some of which cases the chatbot, when asked about women's rights, responded, "I do not think they are so important." The chatbot would also spew out hate speech towards the LGBTQ community, the disabled and minorities, which has brought to the public attention the issue of AI ethics and discrimination.

These discriminatory outcomes mostly stem from the use of biased datasets. "Iruda" usually attracted users in their 20s and 30s and reflected unrefined conversations between them, thereby being implicit in personal views and social perspectives of specific speakers. For AI systems to be gender-neutral, it is important to ensure the machine learning data go through a refinement process while developers need to consider AI ethics at the designing stage.

Another source of the controversy about "Iruda" relates to "explainable AI." Explainable AI is Artificial Intelligence in which humans can understand the decisions or predictions made by AI and trust the results and outputs. The "Iruda" issue has brought to the atten-

CHAIRPERSON JONG IN YOON

Personal Information Protection Commission of Korea (PIPC)

tion of the public how AI is used to make automated decisions.

The PIPC published in May 2021 a "self-checklist for AI developers and users," raising the awareness of stakeholders about personal information protection and calling on them to abide by the PIPA. The self-checklist sets out statutory obligations and recommendations while also specifying six key data protection principles: legitimacy, safety, transparency, inclusiveness, accountability and fairness.

In addition, a bill to amend the PIPA that was laid before the National Assembly of Korea in September 2021 includes a provision on "data subjects' rights, etc. with regard to automated decision-making." The amendment to the PIPA is aimed at guaranteeing at least individuals' right to respond to the infringement of fundamental rights such as monitoring of and discrimination against specific individuals, taking into account the widespread use of automated decision-making for the purpose of credit checks, recruitment, etc. in line with the advancement of technologies such as AI.

The "Iruda" case should not cause excessive concern over the use of AI, eventually undermining the trust in the technology itself. The case should instead serve as an opportunity to form a social consensus around protecting data subjects from new threats through the ethical use of AI, as well as by making sure the compliance with data protection principles.

Furthermore, it is important to keep pace with the development of AI when it comes to putting appropriate safeguards in place, including not only rights to request an explanation of and object to automated decision-making but also rights to not to be subject to automated decision-making and request human intervention.

Considering circumstances where learning data directly affects AI judgment, it is necessary to develop methodologies and tools to verify machine learning datasets to prevent AI-based automated decision-making from having negative impacts on specific groups by eliminating discriminative elements at the collection stage and minimising bias in the datasets. At the same time, conducting research on explainable AI is also an important task to ensure reliability, so it is necessary to develop technologies capable of verifying algorithms for explainable AI and mitigating bias and prejudice in the datasets.

Biased datasets can lead to discrimination which will then weaken the society. Transparent AI systems that we can rely on should build on fair datasets. Depending on how we shape it, AI will lead us either to utopia of gender equality or to dystopia full of bias and discrimination.

IN CONVERSATION WITH

"PROTECTING AGAINST GENDER-BASED PRIVACY HARMS"

Angelene Falk
Australian Information and Privacy Commissioner, (OAIC)

The right to privacy underpins several fundamental values and facilitates the enjoyment of other human rights. But the right to privacy is not experienced equally, and privacy impacts are not always gender neutral. When our personal information is misused or used in unexpected or unanticipated ways, it can lead not only to individual harms, but to collective societal harms. Unfortunately, these harms can often disproportionately affect women.

Protecting against gender-based privacy harm requires a proactive, holistic approach. This includes regulatory cooperation and implementing privacy protections upfront that consider gender implications, as well as implications for other historically marginalized groups in society.

GENDER-BASED PRIVACY HARMS

New data-driven technologies have exacerbated the potential for gender-based privacy harms. The collection, use and disclosure of personal information in the digital environment can lead to different kinds of privacy harms - including physical, economic, psychological, reputational, and discrimination privacy harms. For example, some data-driven technologies, such as location tracking devices, use personal information in a way that may give rise to physical harms, such as stalking and physical domestic abuse.

We also know that women are at greater risk of cyber abuse and image-based abuse. These psychological and reputational privacy harms can be intensified on data-driven social media and digital platforms, by the algorithms used to disseminate content. Online profiling for targeted advertising can further

lead to privacy discrimination harms, excluding women from markets and opportunities.

PRIVACY BY DESIGN

The diverse range of potentially gendered privacy harms, fuelled by personal information driven economies and technologies, means that a one-size fits all approach is unlikely to see a substantial reduction in harms. It is essential that our privacy laws are fit for purpose in the digital economy.

For organisations, these issues reinforce the need for privacy by design, where gendered privacy impacts of new technologies can be handled proactively. This includes considering how those impacts will be experienced due to gender and by other historically marginalised groups, and how to mitigate these impacts. This should be done on an ongoing basis – from initial planning stages to implementation of new technologies.

REGULATORY COOPERATION

As these issues cut across regulatory frameworks, regulatory cooperation is essential to protecting against gender-based privacy infringements and preventing ongoing harms to individuals and communities.

Regulating emerging technologies requires collaboration and coordination between regulatory bodies in different spheres, given the need for complementary expertise. In recognition of this blurring of traditional regulatory spheres, my office and Australia's competition and consumer, communications and media, and online safety regulators recently formed the Digital Platform Regulators Forum to support a streamlined and cohesive approach to the regulation of digital platforms.

Privacy is not experienced or valued equally. Privacy frameworks must mitigate against gender-based privacy harms that are perpetuated in the digital environment. These issues are complex and require multifaceted approaches, including ensuring laws are fit for purpose to encourage privacy by design to minimise gender-based harms and effective regulatory cooperation to understand and address the issues at stake.

Angelene Falk is the Australian Information Commissioner and Privacy Commissioner. She leads the Office of the Australian Information Commissioner (OAIC) in fulfilling its functions across privacy, freedom of information and government information management. Commissioner Falk is a member of the GPA's Executive Committee and chairs the Strategic Direction Sub-Committee. The OAIC also co-chairs the Digital Citizen and Consumer Working Group which explores cross-regulatory intersections and co-operation.

ANGELENE FALK

Australian Information Commissioner and Privacy Commissioner

MIGRATION, GENDER, AND DATA PROTECTION

José Luis Michelena
ICRC

In 2018, Gabriela and her 16-year-old cousin fled their home in search of safety. They joined the more than two million migrants who have left Central America over the last ten years, attempting to flee violence, reunite with family members or simply seek better opportunities for safe and dignified life. Although afraid, Gabriela and her cousin persevered, knowing there was no other option but to move forward. This mixture of hope and desperation, however, would not be enough to overcome the trauma resulting from sexual violence. Isolated, stigmatized, and depressed, Gabriela and her cousin had no choice but to abandon their onwards journey.

Gabriela's case, unfortunately, is not unique. Many migrants travelling through hostile environments, become exposed to physical harm, sexual violence, exploitation, and the risk of family separation or going missing or dying. Throughout the route, they may be subject to various forms of violence, with many having left their home countries to escape these the very same dangers. Due to the difficulty of accessing essential services while transiting across such insecure terrain, migrants also face greater obstacles to receiving adequate care.

The International Committee of the Red Cross (ICRC) and its Red Cross-Red Crescent Movement partners play a crucial role in responding to many of these unmet needs across Central America and Mexico. With its partners, the ICRC works to identify and safely refer vulnerable migrants to access whatever physical, mental healthcare, protection, or other services required at any stage of their journey.

Each time an individual is referred to another humanitarian organization, however, personal information becomes vulnerable to a host of data and privacy-related risks. Protecting this data is therefore a vital ethical obligation to which all humanitarian actors are bound. In cases of migrants who may have faced sexual violence who could be subjected to further stigma, extortion, or abuse as a result, this is especially relevant. As part of its institutional efforts to modernize its commitment to 'doing no harm', including in the virtual space, the Red

Cross-Red Crescent Movement has taken several steps over the last decade to fortify its data protection standards and practices:

- In 2015, the Movement adopted the Code of Conduct on Personal Data Protection in Restoring Family Links to ensure all members of the Movement meet the same standards for data protection when implementing those activities, including for migrants searching to reconnect with their family members.

- In 2018, the ICRC contributed to the Professional Standards for Protection Work guidelines, producing an entire chapter outlining technical guidance for managing data for protection outcomes. The ICRC currently promotes the use of these standards across several migrant shelters in Mexico.

- In 2022, two Movement resolutions on data protection were adopted: 1) Safeguarding humanitarian data, and 2) A Movement approach to assuring and improving patient safety and quality of care, with emphasis on ensuring patient confidentiality and respect for personal data.

Efforts to ensure adequate data protection are critical to safeguarding confidentiality and creating a safe environment for those who disclose they have experienced violence, such as Gabriella.

After several weeks, Gabriela finally felt comfortable disclosing to the ICRC teams what she had experienced and was referred to a civil society organization in Mexico to get care. By reassuring her that all personal data would be carefully managed and treated confidentially, the ICRC was able to connect her to the needed medical and mental health services she had been hesitant and struggling to reach.

Although Gabriela may still have to deal with the lifelong consequences of the sexual violence she experienced, her ability to safely access adequate care knowing confidentiality and her personal data would be protected helped significantly to reduce some of her immediate fears.

PERSONAL DATA PROTECTION AND GENDER IN AFRICA

MARGUERITE OUEDRAOGO BONANE
Commission de l'Informatiqueet des Libertés Burkina Faso

Gender refers to the roles and responsibilities assigned to men and women, and are shaped by our families, societies, and cultures. These notions are learned and can change with time in certain cultures.

In its gender strategy, in 2019, the West African Economic and Monetary Union (UEMOA), states that « gender is a set of characteristics associated to men and women in a society or in a specific historic and cultural context, which models the social identity of an individual ». In Burkina Faso, in the framework of the elaboration of the national gender strategy 2020-2024, the definition of the concept, which was widely accepted, stipulates that: gender must be analysed under the standpoint of inequalities and disparities between men and women, while examining the different social categories with the objective of reaching greater social justice and an equitable development.

MARGUERITE OUEDRAOGO BONANE
Commission de l'Informatique et des Libertés

Regarding personal data, it means all data, manual or automatized, that allows for the identification of a person, such as health, professional life, family life, fingerprints, etc.

In the 21st century, the question of gender equality and women empowerment is more important than ever. In a time when information and communication technologies are an integral part of our daily lives, turns out that the need to reduce the gender gap, meaning reducing the existing inequalities between men and women in access and control of information technologies, their content and the skills allowing their use.

What can be observed from today's information society is far from being an idyllic vision. Much on the contrary, it reveals deep inequalities, both within nations and different countries in the world where millions of women are excluded from the existing possibilities in terms of access to ICT's.

This phenomenon is particularly acute in developing countries, notably in Africa, which carries consequences over the protection of women's rights in general, but also over the protection of their personal data in a very specific way in the continent.

As victims of cyberbullying, "revenge porn", identity theft, misuse of their personal data to be used for malicious purposes, internet is not a safe space for women.

There are cases where images or videos of women, taken without their consent, are uploaded to sites for publicity, pornography, or trafficking purposes.

At the same time, structural inequalities that encompass certain data are themselves problematic once this data is automated, notably when these are grounds for algorithmic systems.

Such is the case of Amazon, who in 2018 had to abandon its automated human resources solution which privileged hiring of male candidates.

In view of the above it is absolutely necessary to:

- Consolidate the interconnections between IT policies and gender;
- Strengthen the efforts to implement a gender perspective in IT;
- Create consultation frameworks to elaborate strategies to implement a transversal approach to gender perspectives and Information technologies;
- Demystify the technical aspects in favour of the development challenge;
- Include women in information technologies policy-making;
- Raise awareness about the unique challenges women face
- Focus connectivity efforts on adult females and heads of household in underprivileged areas such as: education, credit unions, markets, healthcare, etc.;
- Encourage gender equality in the use of information technologies.

DATA PROTECTION AS A GUARANTEE FOR FEMALE SURVIVORS OF GENDER-BASED VIOLENCE

Mar España
Agencia Española de Protección de Datos

We live in the digital age and with mobile devices we access a multitude of service and store a lot of information. Our geolocation, contact list, call and message list, emails and much more. Protecting and checking the level of privacy of their mobile devices is a vital issue for female victims of gender-based violence.

In addition, cases of digital gender-based violence are becoming more frequent and in a few minutes the information disseminated can reach thousands of people.

Examples of digital violence include harassment on social networks, sextortion, monitoring with spy apps on devices, identity theft, reputational attacks on the internet or threats through social media or instant messaging, etc.

The Agency works intensively and from its competencies to address violence, harassment and the gender digital divide with concrete actions.

The priority channel allows the Agency to be notified of the illegal dissemination of sensitive content and request its removal. It aims to provide a rapid response in exceptionally sensitive situations, such as those involving the dissemination of sexual or violent content. The objective is to establish a communication channel so that the Agency, as an independent authority, can adopt where appropriate, urgent measures to limit the dissemination and access to personal data in especially serious cases such as victims of gender-based violence, abuse or sexual assault and harassment. The effectiveness of this channel

is very high since in 85 % of the cases it manages to remove sensitive contents in a few hours or less than 72 hours.

The microsite "Help for victims of gender-based violence and digital violence" aims to raise awareness about the importance of maintaining the privacy of mobile devices and inform about the need to keep devices protected. A series of simple guidelines are given and the existence of tools to maintain the privacy of the mobile phone is highlighted.

The latest call for the Agency's Awards in June 2022 includes an Initiatives and Best Practices Award for better protection of women from digital violence.

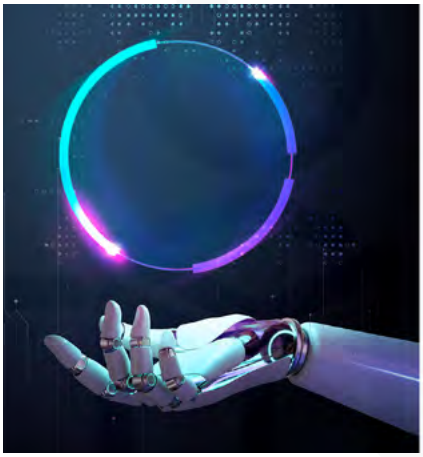
And the Agency's Social Responsibility and Sustainability Policy Framework 2019-2024 includes the "Commitment to Gender Equality", a broad commitment, in multiple aspects of the fight against gender-based violence.

But the supervision work of the Agency is also crucial to guarantee that the processing of personal data that includes data on women victims of gender-based violence, such as the VioGén system (Integrated Monitoring System for Gender-Based Violence), is carried out in accordance with data protection principles, ensuring the exercise of rights and taking measures that minimize the risk to the rights and freedoms of women.

Gender-based violence against women is a scourge, and data protection and privacy provide useful tools to help eradicate it.

The AEPD maintains a firm and concrete commitment to guarantee gender equality, protect victims and, generally protect the rights and freedoms of individuals.

GPA HIGHLIGHTS



WORDS OF APPRECIATION FOR EXCOM DEPARTING MEMBER

On behalf of the Plenary of the National Institute for Transparency, Access to Information, and Personal Data Protection of Mexico we wish to express our sincerest gratitude and admiration to outgoing Executive Committee member Angeline Falk, of the Office of the Australian Information Commissioner for her unwavering support as member of the GPA Executive Committee and Chair of the Strategic Direction Subcommittee.

Commissioner Falk's strategic vision and commitment have been essential in driving forward the GPA's mission of becoming a highly effective global forum for privacy and data protection authorities. Under her leadership, the SDSC took forward the significant work of adopting strategies to increase cross-communication and engagement between the GPA and other important networks and was instrumental in supporting Working Groups to successfully deliver on the Strategic Plan.

SEE YOU IN TÜRKIYE

This year's Global Privacy Assembly is being graciously hosted by our Turkish Data Protection Authority colleagues from 25-28 October in Istanbul. We wish to commend our hosts who have worked hard to prepare a program in line with the mission and vision of the GPA.

We are very happy that for the first time in two years, we will have the opportunity to come together face to face, and we look forward to seeing you in beautiful Istanbul.