DATA PROTECTION & PRIVACY:

A Gender Perspective

July 2022

KICTANet Policy Brief

Supported By

german cooperation
DEUTSCHE ZUSAMMENARBEIT

IMPLEMENTED BY
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

COFUNDED BY EU

KICTANet
The Power of Communities

Published by:

Kenya ICT Action Network (KICTANet)

Email: info@kictanet.orke

Web: www.kictanet.or.ke

Twitter: @kictanet

Programme:

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH- Strengthening Women's Safety Online

Project title:

Strengthening Women's Safety Online

Sponsor:

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Authors:

Prof. Sylvia Kang'ara and Mercy King'ori

Editor:

Victor Kapiyo

Design & Layout:

MediaForce Communications (Email: branding@mfc.ke, Cell: +254 777 665 548)

Photo(Title): TBC

Location: Nairobi, 2022

Year of Publication:

Policy Brief No.12, July 2022

© All parts of this publication may be reproduced freely provided that KICTANet is duly acknowledged

Table of Contents

List of Abbreviations

CMCA - Computer Misuse and Cybercrimes Act. 2018

COVID-19 - Corona Virus Disease 2019

DPA - Data Protection Act, 2019

DPCs - Data Protection Challenges

GPS - Global Positioning System GPS

NGEC - National Gender and Equality Commission

OVAW - Online Violence Against Women

PADVA - Prevention Against Domestic Violence Act, 2015

PwDs - Persons with Disabilities

SDGs - Sustainable Development Goals

SGBV - Sexual Gender Based Violence

SOA - Sexual Offences Act

Executive Summary

Women's online participation presents data protection issues such as lack of agency and control over data, consent in unequal power dynamic contexts, loss of privacy, discrimination, online gender-based violence targeting women and bias that is compounded when age, class and gender intersect. Kenya has been lauded for having a digitally connected and active citizenry, and indeed providing requisite infrastructure, and an enabling environment for digitization has been a policy priority advanced by the government through the ICT Ministry. However, digitization and wide scale online access is but one side of the coin. The other side is exposure to violations of privacy, bias and online violence, which could be suffered by anyone, but women are particularly vulnerable. Women and young girls are harmed differently than other citizens by these violations, an issue not properly addressed by existing policies and laws.

To ensure Kenyan policies and laws are responsive to women's online experiences, this policy brief reviews and identifies gaps in existing policies and laws. By conducting a thorough analysis of the existing law on privacy and documented cases of online privacy violations against women, this brief notes that existing laws and policies were written for a time when virtual participation was not as dominant as it is now. In some cases, what starts as physical privacy and data protection violations do end up becoming Online Violence Against Women (OVAW). However, the law and policies are yet to be comprehensive and coherent enough to grant women all round protection of their rights.

This policy brief notes that Kenya's data protection and privacy rights orientation has four biases that militate against women's online participation: physicality bias, gender neutrality bias, business efficiency bias and a bias favouring executive fiat in public governance. The four biases work together to hamper Kenyan laws and policies from addressing women's unique online experiences. If anything, they replicate online existing social-cultural biases against women. Unless these underlying biases embedded in our institutions change, women shall continue to experience suboptimal online participation, which is inconsistent with the government's stated agenda of inclusivity and digital expansion, and the constitutional right to equality and non-discrimination.

Women's online participation is a worldwide concern, given that internet service is dominated by a few global firms whose platforms are used across national borders. This policy brief focuses mainly on Kenya but also draws from international experiences. The methodology employed is desk review of literature comprising laws, policies, media reports, books, blogs, court decisions and journals. These have been reviewed and analysed to identify the issues and concerns in women's online participation and to determine whether existing laws and policies are adequate. Also captured is information and feedback gathered from KICTANet's earlier policy briefs, webinars and stakeholder engagement forums.

Several recommendations have been presented that formulate the way forward for various government agencies, non-governmental organisations and others focused on solving the problems women experience online. An important recommendation is that it should no longer be assumed that women are safe in online participation just because they are not in physical contact with those who harm them. Perpetrators of OVAW hide behind the cloak of keyboard anonymity. Consequently women can be exactly where society traditionally "expects them to be", namely at home or other 'decent' private space, and still suffer great harm. The old mentality is that women should 'keep a safe distance' and 'be culturally appropriate' to be safe. This frame of mind obviously has no place in modern society in the physical let alone virtual lives of women, and yet, it still influences how people view women's online participation and the unwillingness to hold perpetrators of harm responsible. What is now at stake is not just the female body but something less tangible: data and online privacy (which are invariably an extension of the body).

1.0 Introduction

The fight for women's rights with regards to political, economic and social rights has been fought in many spheres of life, more prominently, in regards to the right to proper healthcare[1] and the right to vote through the universal suffrage movement,[2] among others. One less commonly acknowledged area where women still experience exclusion due to inequalities is in the right to privacy. In fact, the idea of women and their entitlement to privacy is still greatly misunderstood and has for the longest time been seen as two incompatible issues.[3] After its recognition as a common law right, the right to privacy came under sharp scrutiny as a right that is easily accessed and enjoyed by the privileged with women squarely falling out of this category.[4] In their paper *"How Privacy Got its Gender"*, Allen and Mack suggest that the right to privacy as it was originally described by Warren and Brandeis[5] who published one of the most influential articles describing the right to privacy reflects their era's gender bias. They posit that the social context of the origins of the right to privacy happened in an era of sexual inequality and its development has continuously illuminated the inequality and bias of that time.[6]

Privacy was defined by normative assumptions about female modesty, subordination and seclusion. An egalitarian understanding of privacy or one that includes women's freedom to express themselves while still enjoying privacy for their private lives is a recent development.[7] As women's privacy was closely associated with modesty and individual privacy, traditional norms of modesty and domesticity exhibited in speech, dressing and behaviour dominated understandings of a woman's privacy.[8] This expectation of privacy, although outmoded, seems to have informed how women's privacy and private life is handled in modern times and in online spaces as women rely on technology to participate in society.[9] Undoubtedly, this traditional view of women's privacy undermines women's expectation of a meaningful understanding of privacy, one that empowers them, enhances their intimate relationships, and promotes their autonomy.[10] In online spaces, this expectation of privacy, when not adhered to, has seen women subjected to bias, discrimination, technology mediated violence or online violence against women (OVAW), as

1 History of the Women's Health Movement in the 20th Century https://www.jognn.org/article/S0884-2175(15)33790-4/fulltext

2 Universal Suffrage—An Elusive Goal that Leads to The Revolution https://www.loc.gov/exhibitions/women-fight-for-the-vote/about-this-exhibition/seneca-falls-and-building-a-movement-1776-1890/family-friends-and-the-personal-side-of-the-movement/universal-suffrage-an-elusive-goal-that-leads-to-the-revolution/

3 Gender and Privacy in Cyberspace, Anita L. Allen https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1788&context=faculty_scholarship

4 Gender and Privacy in Cyberspace https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1788&context=faculty_scholarship

5 How Privacy Got its Gender,Anita L. Allen https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2309&context=faculty_scholarship

6 How Privacy Got its Gender,Anita L. Allen https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2309&context=faculty_scholarship

7 How Privacy Got its Gender,Anita L. Allen https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2309&context=faculty_scholarship

8 How Privacy Got its Gender,Anita L. Allen https://scholarship.law.upenn.edu/faculty_scholarship/1309/

9 Misogyny online: a short (and brutish) history https://uk.sagepub.com/en-gb/eur/misogyny-online/book245572

10 Technology and Privacy https://www.tandfonline.com/doi/full/10.1080/13511610.2013.768011

commonly understood,[11] collectively referred to here as "data protection challenges (DPCs)".

DPCs have effects on the social, economic and psychological well-being of the victims and are at odds with many governments' efforts to promote equal internet access.[12] Therefore, this realisation of the importance of the internet, whose access has been elevated to the level of a fundamental human right[13] has prompted legislative interventions and adaptation of existing laws to deal with DPCs at the international level, such as the Budapest Convention and at the national level through comprehensive data protection laws. The efforts to accommodate DPCs within existing legal frameworks recognises the significance of the internet as an enabler of other fundamental human rights for women such as the freedom of expression. In Kenya, the right to information privacy is guaranteed under article 31 (c) and (d) of the Constitution of Kenya, 2010 which states that "every person has the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed". To effect this right, the Data Protection Act, 2019 (DPA) was enacted.

This policy brief explores the policy and legislative gaps in data protection that enhance gender bias, that is different treatment of men and women, and focuses mainly on young women. It does so by first, locating women's entitlement to the right to privacy and data protection within Kenya's legal framework, followed by providing a situational analysis of the DPCs that women face using reported incidents in the country. This is followed by an exposition of the policy and legal framework, focused on women and their capacity to deal with the DPCs.

> **"every person has the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communications infringed".**

Particular attention is given to the DPA as the main law that governs collection and use of personal data in the country. In discussing the DPA, the policy brief describes how the DPA could be leveraged to stymy the stated DPCs along with the limitations of applying it in these situations. It reveals that the DPA is a double edged-sword in dealing with the DPCs. Finally, the policy brief concludes with actionable recommendations to policy makers and other stakeholders on concrete steps to be undertaken to deal with the data protection related challenges that women face online.

1.1 Locating Women's Need for Privacy and Data Protection

The framework for examining the right to privacy and women's entitlement to it is found under Article 27 of the Constitution on equality and discrimination that guarantees every person's equality before the law. It provides that every person has the right to equal protection and equal benefit of the law.[14] It further describes equality as the full and *equal* enjoyment of all rights and fundamental freedoms. Since the right to privacy forms part of the rights under the law, women too are entitled to fully and equally enjoy this right without discrimination.

The importance of privacy especially in the online environment cannot be overemphasised. While not an absolute right, privacy is essential to the free development of a person's personality and identity. It is a right that goes to the innate dignity of the person, and facilitates the enjoyment of other human rights.[15] Privacy is also a necessary precondition for the protection of fundamental human values including autonomy, dignity, equality, and freedom from government intrusion. The

11 Online violence against women as an obstacle to gender equality: a critical view from Europe http://oro.open.ac.uk/71877/1/EELR%20 1-2020-Article%20GE%20Online%20violence%20(ORO).pdf

12 Many countries have pledged to fulfil global goals of developments such as the Sustainable Development Goals. Particularly, SDG 9 focuses on investing in ICT access for promotion of peace.

13 U.N. Report Declares Internet Access a Human Right https://www.wired.com/2011/06/internet-a-human-right/

14 Article 27 of the Constitution of Kenya, 2010

15 The General Assembly, the UN High Commissioner for Human Rights and special procedure mandate holders have recognised privacy as a gateway to the enjoyment of other rights (UNGA resolution 68/167, A/HRC/13/37; Human Rights Council resolution 20/8).

right to privacy constitutes a bundle of rights - right to solitude, intimacy and confidentiality[16] that permit having agency over one›s body, ability to control one's identity, room to speak one's mind safely and securely. Where a person validly consents to revealing personal data about themselves, data protection governs what information about them is shared, how it is shared and who receives the data thus making the internet a safe space for women as it continues to revolutionise how they work and interact with other people.

Women currently operate in cyberspace for reasons of convenience and pleasure as well as necessity. A look into the demographic composition of social media platforms such as Instagram indicates that women form a high proportion of users.[17] For some women, such platforms have created opportunities for economic empowerment by providing a platform for them to market their businesses.[18]

The internet has emerged as an important source of news as well as a key platform for disseminating news from the mundane to the latest news".

Beyond economic empowerment, the internet and applications built on it have contributed to social empowerment of women through advocacy efforts that are initiated online.[19] The internet has provided powerful opportunities for online campaigning, activism and protests.[20] By using the internet to demand change in political processes, women are seen to be defying patriarchal stereotypes that dominated such spaces.[21] This is visible among Kenyan women politicians[22] who are leveraging social media to make their voices heard. According to Nanjala Nyabola in her book "Digital Democracy Analogue Politics", "social media has invigorated feminist discourse in Kenya".[23] Beyond female politicians, female human rights defenders and journalists constitute another group of women who rely on the internet to perform their duties. The internet has emerged as an important source of news as well as a key platform for disseminating news from the mundane to the latest news. Similarly, human rights defenders rely on the internet to mobilise people, coordinate their activities, uncover and document abuses.

For all these groups of women, privacy rights ensure that their participation on the internet is safe and secure. Distinctly, female journalists and human rights defenders rely on the internet as it guarantees privacy and anonymity compared to physical spaces due to the sensitive nature of their work. Nonetheless, even for women who rely on the internet for its accessibility and visibility such as business owners and ordinary users, privacy and data protection remains paramount for thriving in this space.

When women's privacy needs are not met, the effects are wide-ranging:

1. Despite its perceived invisibility, online violations of privacy leave behind real and sometimes physical marks. At the online level, privacy violations result in limited uptake of digital technologies thus excluding women from the immense benefits of the internet. This exclusion also runs counter to many global development goals that seek to promote

16 Feminism, Democracy and the Right to Privacy http://www.minerva.mic.ul.ie/vol9/Feminism.html

17 Distribution of Instagram users worldwide as of January 2022, by gender https://www.statista.com/statistics/802776/distribution-of-users-on-instagram-worldwide-gender/

18 Investigating the Impact of Instagram on Women Entrepreneurs' Empowerment https://www.atlantis-press.com/article/125942355.pdf

19 Women's online advocacy campaigns for political participation in Nigeria and Ghana https://www.tandfonline.com/doi/abs/10.1080/17405904.2021.1999287?journalCode=rcds20

20 Feminist Internet: What did we Achieve from 2016-2019? https://www.apc.org/en/news/feminist-internet-what-did-we-achieve-2016-2019

21 Women's Online Advocacy Campaigns for Political Participation in Nigeria and Ghana, Innocent Chiluwa https://www.tandfonline.com/doi/abs/10.1080/17405904.2021.1999287?journalCode=rcds20

22 Senator Susan Kihika's Twitter profile https://twitter.com/susankihika?lang=en

23 Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya (African Arguments) https://blogs.lse.ac.uk/lsereviewofbooks/2018/12/07/book-review-digital-democracy-analogue-politics-how-the-internet-era-is-transforming-kenya-by-nanjala-nyabola/

adoption of digital technologies such as the Sustainable Development Goals (SDGs).

2. When privacy is breached, it has negative implications on the social, economic and psychological state of the victims.24 This is because it exposes them to gendered online forms of aggression that lead to social perils such as bias, harassment and discrimination due to privacy violations. Additionally, it increases a woman's vulnerability as their private data can be used to attack and harass them.

3. When privacy is violated, the risk of surveillance increases. Several factors determine who is being watched or not - socioeconomic status and identity. While surveillance and data exploitation affect all of us, women experience unique challenges owing to entrenched systems of oppression. Cases and reports indicate that women are more likely to be surveilled with harmful consequences making privacy a right that is not equally distributed and one that can be curtailed unlawfully and disproportionately. For example, female journalists are more likely to be subjected to surveillance through technologies such as Global Positioning System (GPS) tracking that facilitate collection of their personal data.25

1.2 Situational Analysis of Women's Data Protection Challenges

a. Nature of Data Protection Challenges

An analysis of the typology of data protection challenges (hereinafter referred to as "DPCs") that women face online indicate that there are potentially three main sources of these challenges: fellow internet users, government authorities and online service providers/ platform providers. This distinction is crucial as the DPCs raised by the different sources are varied but have similar roots in structural inequalities in societies that have contributed to gendered power relations between men and women.[26]

1.2.1 Fellow Internet Users

The importance of the internet in day to day life has seen it resemble a public space akin to the physical world where people interact with each other for various reasons. While neither men nor women can attain complete privacy in cyberspace, women suffer disproportionately when faced by violations of their right to privacy. In some cases, privacy violations against women have translated into physical harm.[27]

For most women, violations of privacy online can be from male[28] partners, ex-partners, colleagues

24 Minding the Gaps: Identifying Strategies to Address Gender-Based Violence in Kenya https://www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/Policy_Brief_on_Gender_Based_Cyber_Violence_in_Kenya.pdf

25 Women Journalists Digital Security http://amwik.org/wp-content/uploads/2018/02/Women-Journalists-Digital-Security.pdf

26 Technology and Violence Against Women www.emerald.com/insight/content/doi/10.1108/978-1-78769-955-720201026/full/html

27 Disembodied Data and Corporeal Violation: Our Gendered Privacy Law Priorities and Preoccupations https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390936

28 Women and Cybercrime: The Dark Side of ICTs www.kictanet.or.ke/Activities/Women-and-CyberCrime-in-KE/Kenya_Study-Women-and-Cybercrime-2nd-Edition-2013.pdf

on the internet or as is the case in many instances, anonymous people on the internet.[29] Common forms of privacy violations in these situations include: revenge porn,[30] cyberharassment,[31] cyberstalking,[32] manipulation of personal information, including images and videos[33] and doxxing.[34] These forms of violations involve releasing private data of women in a bid to shame the victim and to correct "wayward" behaviour. These actions are informed by the misguided notion that women who behave contrary to social expectations of privacy relating to female modesty and domestic seclusion need to be subjected to uncouth "corrective measures" and attacks as part of forcing adherence to the aforementioned expected notions of privacy.

One case of such violations witnessed in 2020 involved a renowned female journalist, Yvonne Okwara, whose mistake was openly defending the first patient to recover from COVID-19, Brenda. When the President of Kenya invited Brenda and Brian (another patient who also recovered from COVID-19) for a press briefing as a means of creating awareness on the disease, netizens could not help but vilify her following concerns that her appearance was a mere public relations stunt in addition to her denying any relations with Brian.[35] One of the notable privacy violations that Brenda was subjected to included having her intimate photos shared online without her consent. Yvonne intervened, reprimanding those who were attacking Brenda. As was the case with Brenda, she was not spared the social media heat. In a growing trend among netizens in Kenya, "receipts" (a loose term to describe evidence on an event or a person's life) on Yvonne's personal and intimate life also began to surface on the internet. This major incident is representative of many other cases that go unreported due to the practical challenges of dealing with DPCs facing women.

1.2.2 Government authorities

a. Law Enforcement

Law enforcement bodies are tasked with the duty of safeguarding the rights of every citizen through enforcement of the law. However, incidents of violation of women's privacy rights by law enforcement officers have been reported. This is double jeopardy for women because it means that the very people in charge of enforcing the law are flippant about their obligations, which explains women's hesitance to report violations to police. Women are hampered in their quest for justice at the courts if they do not have police reports to substantiate their complaints, more so if the police themselves are perpetrators of the offences. The case of *MWK v Another v Attorney General & 3 Others*[36] reveals this lesser known perpetrator of privacy violations against women. In 2015 when Kenyan police arrested unruly students aboard a *matatu,* they strip searched a female form 4 student who was 18 years old at the time the vehicle was intercepted. They searched her undergarments looking for drugs. During the search process, photographs of her naked body were taken and later circulated on social media platforms. She sued the police. Two notable civil society organisations, namely Cradle Children's Foundation and the Independent Medical Legal Unit (IMLU) also joined the suit.

In deciding the matter, Justice John Mativo affirmed her right to dignity and privacy pointing out that, "A strip search is generally humiliating, uncomfortable, and of an invasive nature, and in the instant case it affected the dignity of the girls and in particular the first Petitioner. The photographs annexed to the petition attest to this. The right to dignity is at the heart of the Constitution. It is the basis of many other rights. The basis is that of recognizing that every person has worth and value and must be treated with dignity."

The Judge also pointed out that, "There exists in this case the reasonable privacy interest of the 1st Petitioner who was depicted in the images. There is also a significant public interest in ensuring that no duplication or distribution occurred in the disclosure process. Those interests ought not to have been further compromised by the copying, viewing, circulation or distribution of the images beyond what was reasonably necessary to give effect to her constitutional rights." Justice Mativo further noted that, "Even if the police desired to gather evidence, they ought to have done it within the confines of the law. The chief purpose of the statutory provisions prescribing the manner in

29 Cyberviolence against Women https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

30 Revenge Porn: The Facts https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/405286/revenge-porn-factsheet.pdf

31 Cyberviolence against Women https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

32 Cyberviolence against Women https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

33 Women and cybercrime in Kenya: the dark side of ICTS https://www.kictanet.or.ke/Activities/Women-and-CyberCrime-in-KE/Kenya_Study-Women-and-Cybercrime-2nd-Edition-2013.pdf

34 Protect Yourself from "Doxxing" https://ethics.berkeley.edu/privacy/protect-yourself-doxxing#:~:text=Doxxing%20refers%20to%20the%20collection,shame%20or%20embarrass%20the%20user.

35 Kenyans Turn Against Yvone Okwara after TV Rant (Video) https://www.kenyans.co.ke/news/51614-kenyans-turn-against-yvonne-okwara-after-tv-rant-video

36 M W K v another v Attorney General & 3 others [2017] eKLR. http://kenyalaw.org/caselaw/cases/view/145769/. 20 April 2022.

which women were to be searched was to protect their dignity, humanity and integrity."

> **A child whose nude images are circulated in the media has to go through life knowing that the image is probably circulating within the mass distribution network for the public to see."**

Characterising specifically the harm caused by online distribution of the images of a female child, Justice Mativo said, "A child whose nude images are circulated in the media has to go through life knowing that the image is probably circulating within the mass distribution network for the public to see. This experience may haunt him or her for long because it creates a permanent record of the child's image. The psychological harm to the child is exacerbated if he or she knows that the photograph continues to circulate among viewers who may use it to derive sexual satisfaction or other purposes."

To reinforce the importance of privacy to preserve dignity the judge stated that "The photographing and publication of the child›s images strikes at the dignity of the child, it is harmful to the child, and it is potentially harmful because it invades her privacy and dignity. Dignity is a founding value of our Constitution. It informs most if not all of the rights in the Bill of Rights and for that reason is of central significance in the limitations analysis. The value of dignity in our Constitutional framework cannot therefore be doubted. The Constitution asserts dignity to contradict our past in which human dignity was routinely and cruelly denied. It asserts it too to inform the future, to invest in our democracy and respect for the intrinsic worth of all human beings."

This case is significant as it reveals the possible gender insensitivity by law enforcement authorities who are supposed to protect women in such cases. It amplifies the existing challenge that women still face when reporting physical gender based violence at police stations despite innovations such dedicated gender police desks. [37] If authorities have not fully grasped the challenges of investigating and prosecuting physical gender based violence, as seen in some instances, it would be that much more surprising for them to do any better with the much less appreciated and understood yet widely prevalent violation of women's right to privacy online. Beyond police insensitivity to the plight of women online, a recurring concern is whether they are equipped with knowledge and tools to effectively respond to the DPCs even from fellow internet users as depicted above.

b. Investigation Authorities

Recently, the High Court held that failure by the state to investigate sexual and gender-based violence during the post-election violence in 2017 was a constitutional violation.[38] The court faulted the state for its failure to conduct independent and effective investigations and prosecutions of SGBV-related crimes during the post-election violence. The court added that the failure was also a violation of the positive obligation on the Kenyan State to investigate and prosecute violations of the rights to life, the prohibition of torture, inhuman and degrading treatment, security of the person. General damages of Kshs. 4 million was awarded to each of the petitioners for the constitutional violations. Although the case does not relate to violations of online privacy, it points to weaknesses within the investigative bodies to investigate and prosecute physical cases that could be transposed to instances of online violence against womens where the situation presents itself.

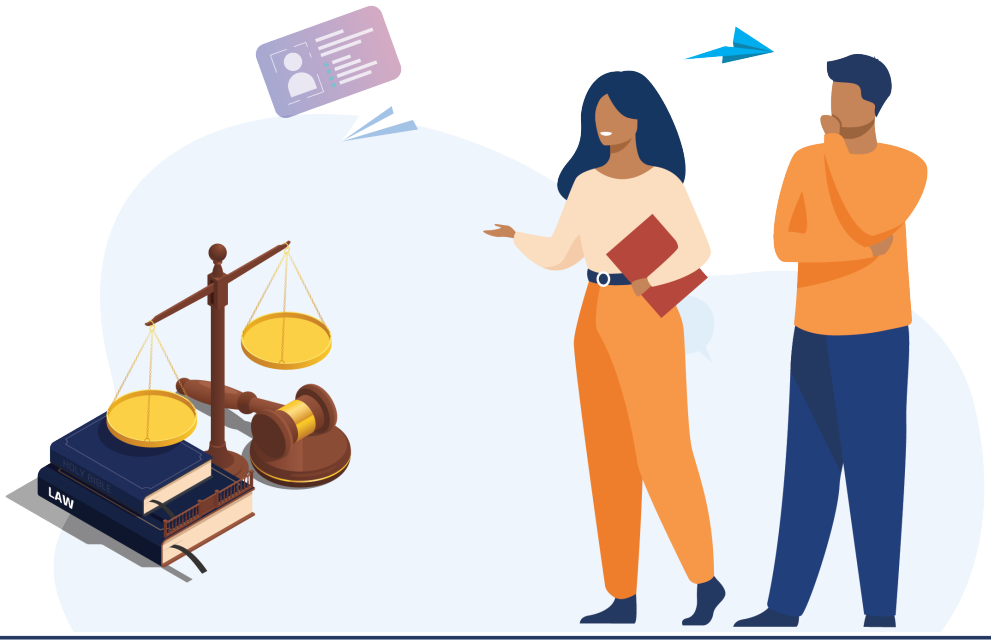
37 Status of Gender Desks at Police Stations in Kenya https://ieakenya.or.ke/download/status-of-gender-desks-at-police-stations-in-kenya/

38 Coalition on Violence Against Women & 11 others v Attorney General of the Republic of Kenya & 5 others; Kenya Human Rights Commission(Interested Party); Kenya National Commission on Human Rights & 3 others(Amicus Curiae) [2020] eKLR. http://kenyalaw.org/caselaw/cases/view/206218/. 20 April 2022.

1.2.3 Online Service Providers/Platform Providers

In addition to violations perpetrated by fellow internet users and government authorities, women face DPCs due to the action or inaction of online service providers. These include the collection of excessive personal data, failing to obtain informed consent and to put in place the necessary security safeguards to protect personal data. These violations have been highlighted mainly in applications that focus on women's sexual and reproductive health. A study done by Privacy International that analysed six popular menstruation apps, some commonly used by Kenyan women, revealed that these applications do not comply with data protection principles such as transparency as well as consent.[39] The report found that these applications share intimate personal data of the users with third parties.

39 No Body›s Business But Mine: How Menstruation Apps Are Sharing Your Data, https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data



2.0 Policy and Legal Framework

2.1 Policy Framework

Kenya has not articulated a policy framework specific to women's online participation and the privacy and data protection problems it exposes them to. However, it has several women›s rights and empowerment policies that offer useful starting points for filling these gender specific policy gaps: the **National Policy on Gender and Development (2019),** the **National Policy for Prevention and Response to Gender Based Violence (2014)** and the **National ICT Policy (2019)**. Three additional ICT policy documents are useful for understanding policy reasons and projections that affect women's online experiences: **Kenya Vision 2030 Third Medium Term Plan 2018-2022**, **Digital Economy Blueprint (2019)**, and the **National Digital Master Plan 2022-2032.**

2.1.1 National Policy on Gender and Development, 201940

The main goal of the *National Policy on Gender and Development (Sessional Paper No. 2 of 2019)* is the achievement of gender equality and women's empowerment. It builds on the foundational work that was initiated by the *Gender Policy of 2000* when advances in women's rights were still nascent compared to today. The 2000 Gender Policy, through gender mainstreaming, proposed key legislative changes that saw the advancement of the rights and freedoms of women in numerous ways. Some notable policy and legislative achievements that emerged from it include:

4. Recognised the need for security of tenure for all people including women. Based on this the National Land Policy (2009) recognized women's right to own property on equal basis with men;

5. Amendment of the Kenya Citizenship and Immigration Act, 2011, provision on dual citizenship to allow married Kenyan women to confer citizenship on their husbands carrying foreign citizenship. Previously, only men could confer citizenship on their non-citizen wives.

The 2019 policy advances the women's rights agenda by introducing ICT aspects, acknowledging that the world is changing fast and that women need to be part of such advancements. It acknowledges the persistent problem of gender inequality due to a patriarchal social order well supported by statutes, religious and customary laws and practices.[41] Additionally, it points to the stark fact that the progressive provisions in law that were based on the 2000 policy have not delivered on the quest for gender equality hence the need for a policy that addresses the variety of

40 Government of Kenya, National Policy on Gender and Development (2019), http://psyg.go.ke/wp-content/uploads/2019/12/NATIONAL-POLICY-ON-GENDER-AND-DEVELOPMENT.pdf

41 Sessional Paper No. 02 of 2019 on National Policy on Gender and Development https://repository.kippra.or.ke/bitstream/handle/123456789/554/NATIONAL-POLICY-ON-GENDER-AND-DEVELOPMENT.pdf?sequence=1&isAllowed=y

manifestations of gender discrimination and inequality.[42]

The policy envisions the government placing focus on women's involvement with ICT. It lays huge emphasis on improving women's access to ICTs. This is indeed a good step in the right direction. However, it fails to cater for the growing social challenges that women face once they are on online platforms, such as cyber harassment, which eventually make moot the efforts made to place ICTs in the hands of women. As this policy brief demonstrates above, the biases and inequality that women face in the physical world are now prominently manifest in the online space. As a policy that is meant to provide direction for laws to be made, this gap in acknowledging the online risks such as privacy infringements that women face is dangerous.

Despite this weakness, the policy covers thematic areas that could be interpreted as aimed at improving the online experiences of women. For example, it includes sections on access to justice, intersectional discrimination, sexual and gender-based violence, culture and behavioral change, which apply in varying degrees to the DPCs that women face online.

2.1.2 National Policy for Prevention and Response to Gender Based Violence (2014)

This policy,[43] currently under review, advocates for a coordinated multisectoral approach towards management of GBV to ensure sustainable GBV prevention and intervention mechanisms as well as enhanced enforcement of law and policies towards GBV.[44] As it currently is, the policy does not envision online forms of violence against women and thus contains no response mechanisms for this underreported form of violence. However, the policy provides important definitions and analysis of GBV. For instance, it is robust since it recognizes emotional violence as a form of GBV, rejecting the idea that GBV is restricted to physical assault. Online violence may culminate in physical violence, or it may follow incidences of emotional violence, for instance where a recording of assault goes viral. By including emotional violence as a form of GBV, the policy provides a useful starting point for incorporating online violence as a form of GBV. Furthermore, the policy recognizes as a type of GBV socio-economic violence, which it describes as denial of services and opportunities, exclusion and ostracization. This definition captures what happens to women when faced by online DPCs.

2.1.3 National ICT Policies

The **National ICT Policy (2019)**[45] is the main policy instrument that highlights ICT related priorities in Kenya that seek to spur the country into an industrialised information society and knowledge economy. With regards to women, the policy provides that the state shall seek to provide an all-inclusive ICT environment by encouraging equality and accessibility. It is therefore cast in general terms and does not address directly the question at hand, namely, women's online experiences including gender-based bias and violence.

The 2019 policy replaces the earlier ICT Policy of March 2006. It places more emphasis on improvement of ICT infrastructure in Kenya and less emphasis on social impact of these ICT infrastructure, this despite having dedicated sections on certain vulnerable groups like children and persons with disabilities, and no dedicated section on women. For example, for Persons with Disabilities (PwDs) the policy focuses mainly on accessibility, which is indeed a crucial matter, but it does not address the social risks that people may face arising from their use of accessible ICTs, such as the risk of human trafficking. As it is, the form and substance of the ICT policy does not yet provide a proper framework to ensure safe online spaces for women.

This infrastructure-first approach taken by the policy comes with the risk that women in the country may eventually have access to the internet and related ICTs but will continue to experience exclusion due to a hostile environment. The net effect of this will see women curtailed from fully enjoying the benefits of being online. As the risk to women's privacy discussed in this policy brief shows, the trend of policymakers leaving out the social impacts in the initial design of policy should not continue to be the case.

42 Sessional Paper No. 02 of 2019 on National Policy on Gender and Development https://repository.kippra.or.ke/bitstream/handle/123456789/554/NATIONAL-POLICY-ON-GENDER-AND-DEVELOPMENT.pdf?sequence=1&isAllowed=y

43 Government of Kenya, National Policy for Prevention and Response to Gender Based Violence (2014), http://psyg.go.ke/docs/National%20Policy%20on%20prevention%20and%20Response%20to%20Gender%20Based%20Violence.pdf.

44 National Policy for Prevention and and Response to Gender Based Violence http://psyg.go.ke/docs/National%20Policy%20on%20prevention%20and%20Response%20to%20Gender%20Based%20Violence.pdf

45 Government of Kenya, Information, Communications and Technology Policy 2019, https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf.

In the development blueprint, **Kenya Vision 2030 Third Medium Term Plan 2018-2022**[46] developing ICT infrastructure is an important policy objective of the government. As with the Digital Blueprint, Vision 2030 TMTP considers ICT infrastructure important to economic development because it will attract global industry and help create high quality and hi-tech jobs in the country. The commitment to create jobs is stated as follows: "In the next five years we will also put in place measures to create over 1 million online jobs for our youths through the on-going Ajira Digital Programme. We will strengthen the institutional framework to support creative arts so that the industry can generate wealth and jobs for our youth." In line with the provisions of the Constitution, the government also demonstrates its commitment to gender equality and gender mainstreaming through allocation of funds designated for affirmative action and gender empowerment, creating employment opportunities, appointment of women in key positions, legislative reform, among other interventions.

Under the National ICT Human Capital and Workforce Development Programme, the government has formulated a Citizen Digital Literacy Programme to make it possible and easier for citizens to interact with the government and receive government services. One of the challenges identified impeding the implementation of government policy on women is inadequate gender disaggregated data, without which formulation of policy, planning, and budgeting with regard to women is hampered. The government is a huge repository of data. The plan makes provision for data collection adequacy in various government departments, data storage in the National Data Centre and data informed policy making and service delivery across institutions. Access to digital infrastructure for women in rural areas makes their experience markedly different from that of women in urban areas.

> **"One of the challenges identified impeding the implementation of government policy on women is inadequate gender disaggregated data, without which formulation of policy, planning, and budgeting with regard to women is hampered."**

Further, Kenya's **Digital Economy Blueprint**[47] was launched by the ICT Ministry in 2019. The Blueprint identifies five pillars of Kenya's digital economy: digital government, business, infrastructure, innovative entrepreneurship, and skills and values. Women's online participation challenges arise in each of the five. Consequently the Blueprint is an important policy document that sets the stage for discussions specific to women's digital experiences. The Blueprint reiterates the government's commitment to a digital economy that is "premised on ubiquitous provision of universal broadband access…" With universal broadband access comes problems of cybersecurity and data privacy, and this is well recognized in the Blueprint, which states, "Data security and informational autonomy are important cornerstones of our democracy, and at the same time a prerequisite for the acceptability and success of a data-driven economy". On the issue of privacy the Blueprint casts a wide net when it states, " It is the task of the many participants in this technology to work together to guarantee trust, security and data protection in an increasingly digitised world. Not only the government, but also business, the scientific community and ultimately the users themselves must contribute to this."

In April of this year, the **National Digital Master Plan 2022-2032**[48] was unveiled by the ICT Ministry. Its key focus is digital integration of service delivery and therefore carries forward policies developed earlier. It incorporates emerging technologies such as blockchain, internet of things, artificial intelligence, big data and quantum computing.

46 Government of Kenya, Third Medium Term Plan 2018 – 2022 Transforming Lives: Advancing Socio-Economic Development through the "Big Four" http://vision2030.go.ke/wp-content/uploads/2019/01/THIRD-MEDIUM-TERM-PLAN-2018-2022.pdf.

47 Government of Kenya, Digital Economy Blueprint, https://www.ict.go.ke/wp-content/uploads/2019/05/Kenya-Digital-Economy-2019.pdf.

48 See Ten-Year National Digital Master Plan Unveiled https://www.kenyanews.go.ke/ten-year-national-digital-master-plan-unveiled/

2.2 Legal Framework

2.2.1 The Constitution and International Treaties

Since the passing of the Constitution of Kenya 2010,[49] Kenya is now operating under a new constitutional dispensation which gives prominence to human rights including the principles of gender equality and nondiscrimination. The Constitution of Kenya contains important commitments to gender equality and women's empowerment as dictated by continental and international instruments that Kenya is party to:

- Article 2 enumerates that the Constitution is the supreme law of the land and any laws that are inconsistent with it are null and void, including customary laws. Women's online experiences including discrimination, harassment and violence are sometimes a carryover from customary and cultural practices within our communities. It is important to point out that retrogressive customary practices and bias are not condoned by the Constitution in physical as well as virtual spaces.
- Article 10 provides an expansive articulation of national values and principles of governance that bind state officers and state organs in the performance of their duties and when making public policy decisions such as equality, human rights and non-discrimination.
- The Bill of Rights specifies the fundamental rights and freedoms of citizens. Importantly, the provisions of the Bill of Rights bind the state as much as they bind private actors, corporations, and firms. This is important to underscore because most internet platforms are predominantly privately owned entities. Notably, just like the state, they too owe constitutional duties to ensure women's online experience is rights-respecting.
    - Article 27 specifically provides for equality and freedom from discrimination as a fundamental right. Equality is defined as the full and equal enjoyment of all rights and fundamental freedoms. Particularly, Article 27(3) provides that women and men are entitled to equal treatment including the right to equal opportunities in political, economic, cultural and social spheres. To ensure that such equal treatment is accorded, the state is mandated to take legislative measures to redress inequality.
    - Article 31 protects the right to privacy and is critical to women in that it creates data protection obligations directed to people and entities handling personal data, including sensitive data.
    - Article 2 makes international treaties part of Kenyan law. Kenya is a state party to human rights instruments that have gender equality and non-discrimination provisions including the Protocol to the African Charter on Human and People's Rights on the Rights of Women in Africa (Maputo Protocol)(2003),50 the International Covenant on Civil and Political Rights (ICCPR)(1966)51 and the Convention on the Elimination of All Discrimination Against Women (CEDAW)(1979)52.
    - The United Nations Sustainable Development Goals (UNSDG)53 are the heart of the 2030 Agenda for Sustainable Development adopted in 2015. There are seventeen goals that include goal 9 on industry, innovation and infrastructure, goal 10 on reduced inequality, goal 16 on peace, justice and strong institutions and goal 17 on partnerships for the goals. These goals are implemented to advance the agenda of poverty reduction and sustainable development. Within this framework, the United Nations Development Group has published a guidance note on data privacy, ethics and protection whose concern is big data collected by private entities and whose mission is to provide member states with a framework for strengthening their Agenda 2030 operational programmes.54 The note seeks to support the use of big data while providing a risk management tool that takes into account fundamental human rights. It sets out nine data protection principles and provides technical definitions to important terms such as consent and data aggregation by gender and other

49 See Constitution of Kenya, 2010 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=Const2010

50 African Union, Protocol to the African Charter on Human and People's Rights on the Rights of Women in Africa (Maputo Protocol) (2003), Article II. https://au.int/sites/default/files/treaties/37077-treaty-charter_on_rights_of_women_in_africa.pdf

51 United Nations, International Covenant on Civil and Political Rights (1966), Article 3 on equality and Article 17 on privacy. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

52 United Nations, Convention on the Elimination of All Discrimination Against Women (CEDAW)(1979). https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm

53 UN Sustainable Development Goals, https://sdgs.un.org/goals.

54 United Nations Development Group, Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda, https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.

classifications. One sees these principles adopted in our DPA.

- The Beijing Platform for Action 199555 was an important milestone that articulated international women's rights and provided roadmaps for gender mainstreaming in domestic national policies and laws. It covered nine pillars of action including violence against women, women and the media, education and training, women and the economy and the human rights of women. National implementation reviews of these areas have been done every five years since. It is noteworthy that the UN Conference on Women held in Beijing was one of four UN conferences on women and it served as a forum for the integration of the agreements reached in previous conferences. The third conference was held in Nairobi, Kenya, in 1985, ten years prior.
- The Declaration of Principles on Freedom of Expression and Access to Information in Africa was adopted by the African Commission Human and Peoples' Rights in 2019 to affirm the provisions of Article 9 of the African Charter which guarantees the right to access and disseminate information.56 In its preamble, it recognizes "the role of new digital technologies in the realisation of the rights to freedom of expression and access to information and the role of open government data in fostering transparency, efficiency and innovation". Principle 3 and 7 affirms non-discrimination in the exercise of the right to freedom of expression and access to information. Principlel 20.6 of the Declaration states, "States shall take specific measures to ensure the safety of female journalists and media practitioners by addressing gender- specific safety concerns, including sexual and gender-based violence, intimidation and harassment." While Principle 29 promotes proactive disclosure and digital publication of data concerning public matters, Principle 40 guarantees the right to privacy and protection of personal information and sets out specific obligations to be undertaken by states in that regard. Principle 41 sets safeguards for privacy and communication surveillance while Principle 42 requires states to develop domestic legal frameworks for the protection of personal information. Principle 42 also enumerates the data protection and privacy principles states should include in their legal frameworks and the institutions they should create to safeguard data rights and promote legal compliance. In the same spirit of developing legal frameworks, the African Commission developed the Model Law on Access to Information for Africa (2013)57 and the Guidelines on Access to Information and Elections in Africa (2017).58
- The African Union Convention on Cyber Security and Personal Data59 Protection (2014) codifies rules to promote and regulate electronic commerce in African countries. It enumerates private law obligations such as choice of law in electronic transactions. It covers specific requirements for electronic advertising, electronic contracts, their form and authentication, and security of electronic transactions. Chapter II of the Convention is dedicated to personal data protection. It requires states to establish data protection legal laws and establish national data protection institutions. It has elaborate requirements on how these institutions are to carry out their mandates. It enumerates data processing principles and the rights of the data subject. Chapter III is on promoting cyber security and combating cyber crime. States are to develop national cyber security policies and protect Critical Information Infrastructure. The Convention has provisions listing legally recognized cyber crimes and their legal elements. It requires states to recognize the crimes in their domestic legislation. The following, and related crimes, are envisaged as cyber crimes in the Convention: attacks on computer systems, computerised data breach, content related offences and offences relating to electronic message security measures.

55 Beijing Declaration and Platform for Action https://archive.unescwa.org/our-work/beijing-declaration-and-platform-action

56 African Commission Human and Peoples' Rights – Declaration of Principles on Freedom of Expression and Access to Information Africa, Adopted in Banjul, Gambia on 10 November 2019. https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf.

57 African Commission on Human and Peoples Rights, Model Law on Access to Information for Africa (2013), https://www.achpr.org/legalinstruments/detail?id=32

58 African Commission Human and Peoples Rights, Guidelines on Accession to Information and Elections in Africa (2017), https://www.achpr.org/public/Document/file/English/guidelines_on_access_to_information_and_elections_in_africa_eng.pdf

59 African Union Convention on Cybersecurity and Personal Data Protection, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

2.2.2 Computer Misuse and Cybercrimes Act, 2018

The Computer Misuse and Cybercrimes Act, 2018[60] (CMCA) was passed on May 16, 2018. The objective of the Act is to protect the confidentiality and integrity of computer systems, prevent the unlawful use of computer systems, facilitate the detection, investigation, prosecution and punishment of cybercrimes, and facilitate international cooperation in dealing with computer and cybercrime matters. Additionally, the CMCA provides for offences relating to computer systems. Of interest to women and their online safety is the offence of cyber-harassment.

> **"we have not found evidence that women who have experienced forms of cyber-harassment as a result of privacy violations have pursued legal claims under the CMCA leading to the conclusion that women have hesitated to take legal action."**

The Act defines cyber-harassment as wilfully communicating, directly or indirectly, to a person with the intention of causing such person apprehension, fear of violence or damage to that person's property or conduct that detrimentally affects that person or conduct of an indecent nature aimed at affecting the person. The provision of cyberharassment as an offence in the law and its ensuing penalty is important as it is closely linked to violations of privacy aimed at *"detrimentally affecting"* a person, especially when intimate images of a person are shared publicly without consent. The CMCA also legislates other cybercrimes: unauthorised access and related crimes,[61] offences related to publication of false information,[62] offenses related to child pornography[63], wrongful distribution of obscene or intimate images,[64] identity theft and impersonation,[65] interception of electronic messages[66]. The Act establishes a Committee with which owners of computer systems are to report cyber threats.[67] In addition, the Act legislates court issued compensation orders and penalties as a remedy for violations of the Act[68].

While this is commendable, we have not found evidence that women who have experienced forms of cyber-harassment as a result of privacy violations have pursued legal claims under the CMCA leading to the conclusion that women have hesitated to take legal action and this could be because of the institutional challenges identified in this brief. Additional research needs to be carried out to provide clarity why the CMCA has not enjoyed broad uptake with women. This could be attributed to lack of awareness of this important provision and procedures around taking action based on it. More fundamentally, it could also be a reflection of a culture of silence around violence against women and girls and acceptance of violence that characterises gender based violence being transferred online.[69] Also, the history of application of the CMCA could point us into another explanation. Since its initial draft was released and subsequently enacted into law, the CMCA has been criticised as a tool for silencing political opponents of the state more than tackling actual cybercrimes. This is evidenced by the lawsuits involving the CMCA - one major one that sought to repeal 27 provisions of the law[70] as well as numerous lawsuits against individuals to

60 Computer Misuse and Cybercrimes Act, 2018 available at: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018

61 Computer Misuse and Cyber Crimes Act (2018), Section 14-20, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018

62 Ibid, Section 22 and 23.

63 Ibid, Section 24.

64 Ibid, Section 37.

65 Ibid, Section 29.

66 Ibid, Section 31.

67 Ibid, Section 40.

68 Ibid, Section 45 and 46.

69 Generation Equality Forum: Kenya's Road Map for Advancing Gender Equality and Ending All Forms of Gender Based Violence and Female Genital Mutilation by 2026, available at: https://www.icrw.org/wp-content/uploads/2021/06/GEF_Kenya_GBV_roadmap-05.21-web.pdf

70 Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] eKLR http://kenyalaw.org/caselaw/cases/view/191276

infringe on their right to privacy, freedom of expression, speech, opinion and access to information online.[71]

2.2.3 Sexual Offences Act, 2006

The Sexual Offences Act (SOA)[72] defines and describes sexual offences and prescribes punishment. It however limits sexual offences to primarily physical acts therefore excludes many non-physical sexual incidences women in the digital age are exposed to. The SOA consolidated all laws relating to sexual offences and repealed most of the provisions in the Penal Code relating to sexual offences. Particularly, it created the new offence of sexual harassment[73] and introduced minimum mandatory sentences for specific sexual offences. However, the definition of "sexual harassment" as conceived by the law is very limiting and appears to only envision the possibility of sexual harassment in a physical scenario. Cyberspace has given new meaning and context to it with the internet containing rising cases of online sexual harassment as this policy brief indicates.

2.2.4 Protection Against Domestic Violence Act, 2015

This Act[74] provides relief to victims of domestic violence by stipulating protections and redress mechanisms. It defines domestic violence as "any form of violence against a person, threat of violence or imminent danger to that person, by any other person with whom that person is, or has been, in a domestic relationship". It further provides a comprehensive definition of "domestic relationship" under section 4. The comprehensive definition of domestic relationship provides a good basis for dealing with online violence against womenOVAW. This is because online violence that involves privacy violations is in some cases perpetrated by people in a domestic relationship with the victim (but mostly by strangers online). A key feature of the PADVA is protection orders[75] which are issued by a court against perpetrators to protect the victim from further harm and risk of abuse. With the emergence of a new form of domestic violence facilitated by the internet, it will be crucial to find ways to expand the situations in which protection orders are issued to online cases.

2.2.5 National Gender and Equality Commission Act, 2011

The National Gender and Equality Commission Act, 2011[76] establishes the National Gender and Equality Commission (NGEC) that has among its mandates the duty to promote gender equality and freedom from discrimination. Together with the State Department of Gender under the Ministry of Public Service, Youth and Gender, the Commission could increase its scope of work to include protection of women in the online spaces. This is bolseterd by the fact that the NGEC is tasked with the role of overseeing the implementation of the National Monitoring and Evaluation Framework towards the Prevention of and Response to Sexual and Gender Based Violence, 2014.[77]

2.2.6 Kenya National Human Rights Commission Act, 2014

The Kenya National Human Rights Commission Act[78] gives effect to Article 59 of the Constitution which establishes several Independent Constitutional Commissions. At the outset it is important to note that since there also exists the Gender and Equality Commission, the jurisdiction of the KNHRC excludes matters of equality and discrimination, which are to be taken to the former.[79] Further, the Commission's jurisdiction does not include matters pending in a court of law.[80] This means that persons seeking redress for OVAW and other violations must sequence their actions if they want matters addressed by the Commission. The mandate and powers of the Commission are broad ranging from promoting respect for human rights to investigation powers to quasi-judicial powers of issuing summons and getting sworn statements.[81] The Act establishes a complaints mechanism and enumerates procedures for presenting complaints to the Commission.[82] On

71 Kenya Police Turn to Twitter PR as the Arrest of a Blogger goes against Public Opinion. Available at: https://advox.globalvoices.org/2021/03/19/kenya-police-turn-to-twitter-pr-as-the-arrest-of-a-blogger-goes-against-public-opinion/

72 Sexual Offences Act, No.3 of 2006 available at: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%203%20of%202006

73 Ibid, Section 23.

74 Protection Against Domestic Violence Act, 2015 http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%202%20of%202015

75 Ibid, Part II.

76 National Gender and Equality Commission https://www.ngeckenya.org/Downloads/The_National_Gender_and_Equality_Act_2011.pdf

77 National Monitoring and Evaluation Framework towards the Prevention of and Response to Sexual and Gender Based Violence in Kenya, http://www.ngeckenya.org/Downloads/National-ME-Framework-towards-the-Prevention-Response-to-SGBV-in-Kenya.pdf

78 Kenya National Commission on Human Rights Act, No. 14 of 2015. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2014%20of%202011

79 Ibid, Section 30.

80 Ibid, Section 30.

81 Ibid, Section 27.

82 Ibid, Section 32-33.

receiving complaints, the Commission is mandated to report and make recommendations to the authorities legally required to take action.[83]

2.2.6 Data Protection Act, 2019

In 2018, Kenya's Cabinet Secretary for ICT gazetted the establishment and appointment of members of a task force whose mandate was to "develop the policy and regulatory framework for privacy and data protection in Kenya".[84] It is within this context that the Data Protection Act was drafted and eventually passed by Parliament in November 2019. As the law meant to realise the constitutionally guaranteed right to privacy, the DPA can to a large extent be used to tackle rising cases of OVAW. The Act contains certain important provisions, discussed below, that address certain core issues that have led to the prevalence of OVAW including consent and rights of data subjects.

a. Consent

Lack of consent to collect and use the personal data of women has for a long time been a leading cause of violating the right to privacy that sometimes leads to OVAW. The instances of bypassing obtaining consent from a data subject to process their data have been attributed to the existing power imbalances that have for a long time characterised women's lives. On the internet, the provision of valid forms of consent for women has also been interrogated revealing transplanting of offline gendered stereotypes to online space. As mentioned earlier, the case of sexual and reproductive health applications targeting women have come under sharp scrutiny for collecting and using sensitive personal data without valid consent.[85] For these applications, invalid forms of consent have been used to avoid barriers to the circulation of data about our bodies and their profits.

In addition to reinforcing power imbalances, failing to obtain consent from a woman to share her data has been linked to the need to shame and embarrass the victim as is seen in the provided case studies. This non-consensual revelation of private data violates the requirements of consent as provided for under the DPA.

> "...failing to obtain consent from a woman to share her data has been linked to the need to shame and embarrass the victim."

To properly understand the challenges of realising consent among women, it is worth pointing out that they are not unique to the online space. Since time immemorial, obtaining valid forms of consent from women has been met with roadblocks leading to gross violations of women's right to privacy partly due to structural inequalities in societies that have seen gendered power relations affect how informed consent is granted. The case of *I.V. v Bolivia*[86] whose setting was in the healthcare space dealt with the question of informed consent for women. Particularly, the case recognised the power imbalance that existed between the claimant, a woman and health practitioners that led to her forced sterilisation through tubal ligation without her consent. In providing its rationale, the court emphasised on how failure to obtain informed consent due to gender stereotypes and prejudices resulted in privacy infringement of I. V.

83 Ibid, Section 42-43.

84 See Request for comments on the Proposed Privacy and Data Protection Policy and Bill, 2018 https://ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/.

85 Menstruapps: How to Turn your period into Money https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/

86 I.V. v. Bolivia, Preliminary Objection, Merits, Reparations and Costs, Judgment, InterAerican Court of Human Rights (ser. C) No. 329 (November 30, 2016). https://www.corteidh.or.cr/docs/casos/articulos/seriec_329_ing.pdf

According to the DPA,[87] consent is one of the lawful grounds for processing of personal data. The law defines consent as "any manifestation of express, unequivocal, free, specific and informed indication of the data subject›s wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject".[88] It further stipulates that for consent to be lawful, a data subject must be offered control and a genuine choice about accepting or declining the terms offered or declining them without detriment.[89] Valid consent determines how much control of their personal data a data subject enjoys i.e. how their personal data is collected, used and disseminated. When seeking consent, a data controller or processor has the duty of assessing if it will meet the legal requirements of obtaining valid consent. In the absence of valid consent, data processing is unlawful especially if the control provided to the data subject is illusory. In recognition of the importance of consent as a lawful ground of processing personal data, the Office of the Data Protection Commissioner released Guidelines on Consent to provide practical guidance to data processors and data controllers on how to provide valid forms of consent.[90]

If we consider that informed consent to collect and use data is a baseline data protection and privacy law concept, and if we also appreciate that consent is ill-defined and rarely sought, it follows that making a case that results in the award of remedies is an uphill task, despite the DPA providing for remedies and penalties for breach of the Act.[91] The problem of insufficiency of remedies was highlighted by Justice John Mativo in the *MWK* Case[92] discussed above. He noted:

> "**It was self-evident that the assessment of compensation for an injury or loss, which was neither physical nor financial, presented special problems for the judicial process, which aimed to produce results objectively justified by evidence, reason and precedent. Subjective feelings of upset, frustration worry, anxiety, mental distress, fear, grief, anguish, humiliation, unhappiness, stress, depression and so on and the degree of their intensity were incapable of objective proof or of measurement in monetary terms. Translating hurt feelings into hard currency was bound to be an artificial exercise. There was no medium of exchange or market for non-pecuniary losses and their monetary evaluation was a philosophical and policy exercise more than a legal or logical one. The award ought to have been fair and reasonable, fairness being gauged by earlier decisions; but the award ought to also of necessity have been arbitrary or conventional. No money could provide true restitution. Although they were incapable of objective proof or measurement in monetary terms, hurt feelings were none the less real in human terms.**"

In awarding Kshs. 4 million general damages, the judge concluded that the "conduct of searching the 1st Petitioner in the presence of male police officers and/or other students and members of the public and photographing her or allowing or permitting third parties to take her nude photographs was a gross violation of the law and an infringement of her constitutional rights to dignity, privacy and her right not to be subjected to degrading treatment. …. the 1st Petitioner was entitled to damages for violation of her constitutional rights to dignity, degrading treatment and privacy."

b. Sensitive personal data

The DPA categorises certain classes of data as sensitive. Section 2 defines sensitive personal data as data that reveals several things including: a person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details, sex or sexual orientation of the data subject. Part V of the Act further provides the grounds for processing of sensitive personal data. Notably, it prohibits processing of sensitive personal data unless principles of data protection as enumerated under the Act are adhered to. In particular, section 46 provides the grounds on which personal data relating to health may be processed. This is particularly important in the context of women and data protection given the proliferation of women's health applications which collect vast amounts of personal data during operations.

The question of sensitive personal data is also crucial in light of the intersectional nature of

87 Data Protection Act No. 20 of 2014, Section 30 and 32. http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019

88 Section 2, Data Protection Act (2019)

89 Section 32, Data Protection Act (2019)

90 Office of the Data Protection Commissioner, Guidance Note on Consent (2021). https://www.odpc.go.ke/download/odpc-guidance-note-on-consent/

91 Supra, Section 73 on imprisonment, forfeiture and prohibition orders; Section 65 on compensation to data subject for breach of provisions of the Act.

92 Supra note 34.

discrimination that women are likely to be exposed to when such personal data is publicised online. For example, one category of sensitive personal data is one's marital status. Female politicians navigating the online space are best placed to demonstrate how their sex and marital status, two categories of sensitive data place them at a high risk of online violence. Discrimination based on marital status is one representation of the societal basis that women are typically subjected to. This affront to full and equal participation of women in the political arena as it shifts to the online space has seen women opt out of these spaces.[93] The concern of discrimination due to marital status took center stage in the case of *Mary Masinde v County Government of Vihiga*[94]. In this case, Mary Masinde, a married woman was denied a job by the County Government of Vihiga on the basis of "being married" in a neighbouring county. Like other candidates, she saw the job opportunity advertised on an online platform and provided the personal data specified for the job. She was the only female candidate for the job. Male candidates who were not resident in Vihiga were not treated the same way. In deciding the matter, the High Court found that she had been discriminated against on the basis of marital status as she qualified for the job and had demonstrated knowledge of how to do the job.

c. Rights of data subjects

The DPA contains provisions on the rights of data subjects.[95] Particularly, it provides the right to:

- Receive information on the use to which their personal data is to be put
- Access their personal data in custody of data controller or processor
- Object to the processing of all or part of their personal data
- Correction of false or misleading data
- Deletion of false or misleading data about them.

For women, these rights are crucial for their safe participation online. More importantly, though, would be proper and timely enforcement of these rights in times of crisis. The following section expounds on the role of two out of five of these rights in preventing and/or responding to instances of inequality that arise due to power imbalances between technology providers and users. These two are necessary rights that facilitate realisation of other rights. In the same vein, the challenges of realising these rights are discussed.

- Receiving information on the use to which their personal data is to be put

This right imposes on data controllers and processors a duty to inform data subjects how the data that is collected from them is to be used. Section 29(c) re-emphasises this requirement as part of the duty to notify. In most cases, data controllers and processors explain the purpose of collecting personal data through privacy policies which a user of an application is assumed to have read and understood. Having a privacy policy in place for a long time led to the false assumption that an entity has proper privacy requirements in place.96 However, for the longest time now, privacy policies have been criticised for a variety of issues including but not limited to being long and incomprehensible and most importantly, not complying with privacy laws.

- Access their personal data in custody of data controller or processor

The ability of a data subject to access personal data held by a data controller or processor is crucial for reducing the information asymmetry (a component of power imbalances) that may exist between a data controller and a data subject. Through a data subject access request (DSAR), a data subject can obtain the information held about them. The pivotal nature of this right emanates from the fact that awareness of information held by a data controller can allow a data subject to enforce other rights accorded to them such as the right to object to processing of all or part of their data, seek correction of false or misleading data about them or seek deletion of such data. Regulation 8 of the Data Protection (General) Regulations, 2021 provides further guidance to ensure that access requests are effective. Particularly, it constrains data controllers from stifling the right of access through means such as unfair file formats[97] and prohibitive costs[98] while also recognising the risk that access requests may impose on other data subjects.[99]

Beyond ensuring compliance with the law, the right to access data functions as a guarantee for due

93 Understanding Violence against Women in Politics and Leadership: A study on the 2021 Uganda General Elections https://vawp.pollicy.org/
94 Mary Mwaki Masinde v County Government of Vihiga & 2 others [2015] eKLR. http://kenyalaw.org/caselaw/cases/view/111633/. 20 April 2022
95 Section 26, Data Protection Act (2019)
96 A Critique of Consent in Information Privacy https://cis-india.org/internet-governance/blog/a-critique-of-consent-in-information-privacy
97 Regulation 8(3), Data Protection General Regulations, 2021
98 Regulation 8(5), Data Protection General Regulations, 2021
99 Regulation 8(4), Data Protection General Regulations, 2021

process of law. As data is collected as input for decision making on various issues such as targeted advertisements or providing loans, having access to data used in such processes can illuminate concerns of bias and discrimination that may arise.

d. Complaints Handling

Part VIII of the DPA on enforcement provisions provides a solid foundation in case of complaints by a data subject on the manner in which a data processing activity is being carried out. It provides the means of lodging a complaint to the Data Commissioner as well as the timelines of investigation of the complaints.

2.2.7 Limitations of the DPA to deal with DPCs

While data protection norms can serve as a tool to unsettle the power imbalance that contributes to harmful online experiences of women as data is processed thus minimising the risk of surveillance, violence and human rights violations, certain features of the DPA could negatively impact these efforts:

a. Exemptions under the DPA that exempt personal activities from the ambit of the law.

Section 51(2)(a) of the DPA exempts processing of personal data by an individual in the course of a purely personal or household activity from the provisions of the law. However, such processing must adhere to data protection principles of lawful processing. While it is not clear what "personal or household activity" means, other jurisdictions such as the EU which have a similar exemption which could aid in understanding its scope. Recital 18 of the GDPR states that "the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity".[100] It further lists such activities including: correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. In the context of OVAW and how it typically occurs i.e. an abuser sharing private data on social media sites, it would then mean that DPA does not apply unless the information is placed in a public platform, mass media or other context whereby it ceases to be confined to personal or household activities. In those instances, an unlawful transmission or use of the information is legally redressable under the statute. Thus safeguards such as lodging a complaint with the ODPC and conducting investigations as provided under the DPA may not be available to victims of online abuse if the abuse happens in the context of personal, intimate or domestic relationships.

b. Limitations on employing the complaints provisions of the DPA

As mentioned in the previous section, the DPA contains sections on lodging a complaint. However, since the DPA's scope is limited and does not apply to household activities, it means that a data protection complaint in the context of a household setup cannot enjoy these benefits. It appears that only complaints against entities that fall under the formal categories of data controllers or processors can be admitted.

c. DPA assumes order/structure while OVAW reflects the opposite

The structure of the DPA, like many other data protection laws, presupposes order, fixed categories, normalcy and objectivity.[101] This can be seen from the content, structure and procedures in the law. A thorough analysis of the DPA indicates that it is a governance tool aimed at providing guidance for day to day processing of data and less of a law for times of disorder and ambiguity that commonly characterises privacy violations against women. For example, anonymity is viewed as a desirable data protection concept that ensures that personal data is no longer identifiable in the commercial use of data[102] On the other hand, one of the breeding conditions for OVAW is anonymity which allows a perpetrator to hide behind the veil of the internet to expose the private information of others due to the perceived invisibility provided by the internet.

d. Requirement of harm for data protection infringement

The law does not regulate offence, rather it focuses on whether harm has been caused and the remedy for such harm. The DPA includes the "risk of significant harm" as the threshold for events

100 Recital 18, GDPR (2018) https://gdpr-info.eu/recitals/no-18/

101 Feminist Data Protection: an Introduction https://policyreview.info/articles/analysis/feminist-data-protection-introduction#:~:text=11%20The%20protection%20of%20feminist,visualisation%2C%20and%20crowd%2Dsourcing

102 Section 37(2), Data Protection Act (2019)

such as whether to notify the ODPC or a data subject of a data breach.[103] The composition of "real significant harm" has not been described. In the absence of such guidance, it is not clear if that included physical, material, or non-material damage or all of them. This clarification is necessary as the effects of OVAW are not necessarily physical.

e. Low awareness on the applicability of the DPA beyond non-business settings

Despite the close relation of the DPA to tackling OVAW, its full applicability is encumbered in various ways. A poll conducted by Amnesty International in 2021 titled ***The State of Awareness on Data Protection in Kenya***[104] found that while 54% of Kenyans are aware of the right to privacy, 67% are unaware of the DPA. In addition, 53% of Kenyans do not know where to report data privacy violations, while only 18% are aware that there is an Office of the Data Protection Commissioner. The poll also revealed that a high percentage of Kenyans question the efficacy of data protection institutions.

As a discipline, data protection mainly seeks to ensure that personal data of data subjects is collected, processed and used within the limits of appropriate safeguards that are usually articulated in laws and organisational policies.[105] Therefore, in data protection, use of personal data is central to its understanding. This perspective has contributed to data protection being viewed mainly from an economic perspective.[106] Data protection on the internet is largely viewed from the lens of collecting, processing and use of personal data for commercial purposes while maintaining certain security safeguards. The main motivation behind this lies in the growing datafication[107] of daily lives.

One notes that the Data Protection Act is largely oriented to business efficacy where data controllers and processors are given a set of rules on how to collect data and handle collected data. This can be seen in the current wave of awareness efforts by the ODPC towards compliance with the DPA and calls to register as data controllers and processors as required by the law. However, it must be noted that the foremost need for privacy is more than an economic one rather a social need for privacy that is effected through commercial entities. The social perspective of privacy would require a thorough inquiry into how privacy is enjoyed (or not) among various groups of societies including women. The movement towards interrogating the end beneficiaries of privacy has gathered momentum in other parts of the world.[108] This lack of awareness on the foundational role of privacy as a tool for social transformation was evident in the *Nubian Rights Forum* case[109] regarding rolling out Kenya's national digital identity scheme. The case dealt primarily with the exclusionary nature of the proposed system.

According to the petitioners, a minority community in Kenya, the system would exclude them and consequently affect their access to public services. The question of the privacy implications was also raised as a matter of concern for the entire citizenry that had enrolled into the system and not how poor privacy safeguards would particularly affect the minority community. The court in mandating that the DPA be enacted before further processing of data and not elaborating how lack of proper security safeguards of the system amounted to a privacy risk to the community was a missed opportunity to apply the DPA to protect fundamental rights such as protection from bias and discrimination, issues that are in the realm of social justice.

103 Section 43, Data Protection Act (2019)

104 Amnesty International, Still Unaware: The State of Awareness on Data Protection in Kenya https://www.amnestykenya.org/wp-content/uploads/2021/05/State-of-Awareness-Opinion-Poll.pdf

105 https://iapp.org/resources/article/data-protection/

106 Feminist Data Protection: an Introduction https://policyreview.info/articles/analysis/feminist-data-protection-introduction

107 Datafication, Internet Policy Review https://policyreview.info/concepts/datafication

108 Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3806&context=faculty_scholarship

109 Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR http://kenyalaw.org/caselaw/cases/view/189189/

3.0 Conclusions & Recommendations

As women continue to rely on the internet for their social and economic lives, personal data is collected. As seen, this personal data may be used in ways that expose women to various data protection challenges such as bias, discrimination as well as violence. It is therefore instrumental that they are afforded protection by law to ensure that their participation online is safe and secure. This will require a multi-stakeholder approach as different bodies have various roles. At this juncture, it is important to acknowledge the challenge of recommending changes to laws or policies that particularly target women. That notwithstanding, different stakeholders have a role to play to create an ecosystem that can effectively deal with these data related challenges. The following are the recommended pathways that different stakeholders could take:

3.1 Government

- Recognition of OVAW as a form of sexual and gender based violence. In 2021 Kenya unveiled "Kenya's Roadmap for Advancing Gender Equality and Ending All Forms of Gender Based Violence". The roadmap is Kenya's ambitious plan on ending all forms of gender based violence by 2026. However, this goal risks not being achieved if online forms of violence are not recognised and addressed in policy and legislative efforts. For example, one salient benefit of recognising OVAW as a form of gender based violence is that victims may benefit from psychological support services that the government intends to provide as part of committing GBV into the essential minimum package of the Universal Health Coverage. This will be in recognition of the psychological harm that OVAW causes.
- Implement the Guidelines on Consent by mandating compliance with them. A notable feature of the Guidelines is that it mandates data controllers and processors to develop consent processes that respect their statutory obligations as well as the nature of their relationship with the data subjects from whom data is collected. This implies that consent mechanisms need to be adaptable depending on the targeted audience.
- Amend the exemptions under the DPA to cater for OVAW that is conducted through correspondence. This is crucial as it will invoke provisions on complaints handling and investigations by the Data Commissioner in cases of privacy breaches amounting to OVAW.
- The relevant authorities should work collaboratively. OVAW requires multi-agency efforts due to its complex nature. To effectively tackle OVAW the ODPC will be required to work with other government agencies and departments such as the Kenya Computer Incident Report Team under the Communication Authority.
- It will be necessary for law enforcement to be empowered with knowledge on how technologies work which will make collaboration easier, as well as sensitization on handling

sensitive personal data. As seen in the facts adduced in the MWK case, it is clear that the police officers who committed these privacy violations had no training whatsoever on the handling of sensitive images following search and arrest.

- Updating hate speech laws (NCIC Act) to reflect modern realities as brought about by technology. Currently the laws on hate speech in Kenya focus mainly on ethnicity. However, the face of hate speech even in Kenya is changing and now forms part of OVAW.
- Simple, effective and actionable reporting mechanism for OVAW e.g. hotline, special police desk akin to Policare. If well managed, this will increase the proportion of cases reported by women.
- Review the Sexual Offences Act, 2006 to cater for OVAW. Introducing capacity building initiatives for judges to improve their abilities to adjudicate OVAW cases. The Chief Justice of Kenya recently launched the first specialized sexual and gender based violence court in Kenya.[110] This notable achievement should be used as an opportunity to create awareness of the expanded scope of gender based violence due to privacy violations beyond the physical spaces and into the online space.
- Revise policies on gender based violence to cater for OVAW.
- Through the legislative provided powers to initiate investigation into data practices by controllers, the ODPC should begin investigation into the data practices of online services targeted towards women.
- Ratifying the Malabo Convention to create a robust cybersecurity and data protection framework will increase the protection over data that is collected and processed in online spaces.

3.2 Civil Society Organisations

- Engage with the government and other stakeholders to ensure that sound policies are made to recognise and deal with the problem of OVAW. For example, the National Policy for Prevention and Response to Gender Based Violence (2014) is currently under review. The policy recognises the concept of multi-sectoral response to GBV. As GBV assumes a new face in the online space, it is important that mechanisms to engage with stakeholders such as the platform providers are proposed and implemented.
- Provide training to women to empower them to exercise the rights online in the following areas:
    - Cyber security information and education.
    - Fraud detection skills/education.
    - Legal protections for arms length transactions whether governed by statute or contract where women are protected from harm.
    - Ways of correcting data breaches using mechanisms provided by the law.
    - Vulnerability self-assessment, say, depending on one's exposure and work type; getting workplace protection just like all other high risk jobs that require protective gear. For instance is there insurance one can get for online harm just as there would be for highly mechanised jobs?

3.3 Media

The media plays a vital role in increasing awareness of social issues. In terms of OVAW, the media should:

- Increase sensitization on gender issues and the role of societal stereotypes in perpetuating such bias. This will help tackle the underlying basis for most common forms of OVAW.
- Exercising caution during narration and exposition of stories that have a gender lens to it. For the longest time, the issue of victim blaming in stories on gender based violence have had a negative effect on the victims and efforts of dealing with the real issue. Media practitioners should therefore, exercise caution with online cases.

110 Judiciary of Kenya, Launch of the Specialized SGBV Court at Shanzu and Celebration of the UN International Day of Women Judges https://www.judiciary.go.ke/launch-of-the-specialized-sgbv-court-at-shanzu-and-celebration-of-the-un-international-day-of-women-judges/.

- Prioritise the safety of the survivor In cases of violence that arise due to information leakage, the right to dignity and confidentiality of the victim should be taken into consideration.
- Media houses should expand their workplace policies to protect women against this form of violence as well as effective response mechanisms in the event that it happens. Evidence indicates that female journalists are adversely affected by OVAW. The online space is core to the work of journalists; as a source of news and tool for disseminating news.

3.4 Academia

- It is imperative that continuous studies into the nature of OVAW are conducted. This will be important to support evidence based legislative processes. OVAW is a dynamic phenomenon that is not fully understood. As technology evolves so do the risks that are associated with such an evolution. To unearth these risks and how they play out in different facets of society including women,

3.5 Technology Community

- Assess the power dynamics of consent as elaborated and whether the provisions on consent and the ensuing guidelines recognise that in applications.
- Create innovative means of obtaining consent especially in applications targeted at women. As earlier noted the guidelines on consent permits flexibility based on the nature of the relationship of a controller and a data subject.
- Work together with the ODPC to conduct audits of the products, processes and systems compliance with the DPA to ensure that they do not pose data protection risks to women.
- Work with local authorities and bodies to understand the nature and extent of OVAW to ensure that proposed remedies are useful for the various contexts.
- Incorporate privacy by design and security by design into the product development lifecycle.
- Bias and discrimination against women in technology products has been attributed partly due to the lack of representation during development. To deal with this, companies should seek to increase the number of women in the senior roles as well as developer roles.
- As part of increasing implementation of transparency requirements of the law, technology companies should adopt creative ways of explaining to users about a product's data collection practices and provide valid means of enforcing or declining consent.

Follow us on Twitter @KICTANet
www.kictanet.or.ke
Email: info@kictanet.or.ke

Supported By

german cooperation
DEUTSCHE ZUSAMMENARBEIT

IMPLEMENTED BY
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

COFUNDED BY EU

KICTANet
The Power of Communities