Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 4, Issue 1 (2024) p.167-203
https:doi.org/10.52907/jipit.v4i1.505

Privacy in Displacement: Data Protection for Refugees in Sudan

*Teresia M. Munywoki**

ABSTRACT

This paper examines the data protection challenges faced by refugees in Sudan with significant focus on how these challenges disproportionately affect the female refugees. Sudan hosts a significant refugee population; however, it lacks a comprehensive data protection legislation. By focusing on the intersection of gender, refugee status, and digital vulnerability, this paper discusses how the personal data of refugees can be protected. The author highlights identity theft, discrimination, marginalization, privacy breaches, and data exploitation as challenges that arise from the activities of humanitarian organizations within and without refugee camps. As recommendations, the author advocates for effective Data Protection Impact Assessment (DPIA) to be integrated into the activities of humanitarian organizations, enactment and enforcement of a data protection law, and the establishment of a national data protection authority in Sudan. These measures aim to protect the digital rights of refugees and mitigate their exposure to data related risks.

Keywords: Data Protection, Data Protection Impact Assessments, Refugee Women, Humanitarian Organizations, Sudan

* The author is an Advocate of the High Court of Kenya with expertise in ICT law, privacy, and Al governance. She has advised clients on privacy laws, supported clients in regulatory compliance, and has represented parties in matters before the Office of the Data Protection Commissioner. She is also a speaker on emerging digital rights issues and actively champions frameworks for digital rights protection. Email: Teresia.Munywoki36@gmail.com

TABLE OF CONTENTS

I. INTRODUCTION

Sudan has long served as a host country for refugees fleeing conflict in neighboring regions. Presently, it hosts an estimated eight hundred thousand refugees from South Sudan and three hundred and thirty thousand refugees from Syria, Yemen, Central African Republic (CAR), Chad, Eritrea and Ethiopia (WHO, 2024). Women and girls constitute fifty-three percent of this population (ILO, 2024). Notwithstanding that Sudan has a long-standing tradition of providing refuge, it lacks legal frameworks necessary to address the specific vulnerabilities faced by refugees, especially refugee women—particularly in data protection.

Refugees in Sudan face a multitude of legal, linguistic, and social challenges that exacerbate their marginalization, particularly in the context of data protection and privacy (Gehlen et al., 2020). Legal obstacles such as difficulties in obtaining documentation, accessing legal counsel, and understanding their rights in the host country, create significant barriers to securing their personal data (Gehlen et al., 2020). Without proper documentation, refugees may struggle to prove their identity, making them more vulnerable to identity theft and exploitation (Schoemaker et al., 2021). Additionally, their limited access to legal resources further hinders their ability to seek redress in cases of data breaches or privacy violations (Reidenberg, 2002). This lack of legal protection compounds the risks refugees face, as they often have little recourse when their personal information is misused (Gauci at al., 2015).

Shishehgar et al., (2017) argue that while these risks are not exclusive to women, the distinct socio-cultural and economic conditions faced by refugee women in Sudan amplify their vulnerability compared to men. This informs why this paper pays greater focus on how the extant data governance gap in Sudan disproportionately affects refugee women, thereby exacerbating their vulnerability to violations of privacy, identity theft, and ex-

ploitation (Gilman & Green, 2018). In the context of Sudan, a nation hosting a considerable population of refugees, the absence of comprehensive data protection legislation serves to intensify these risks.

Refugee women constitute one of the most vulnerable and marginalized demographics on a global scale, confronting compounded difficulties due to their intersectional identities as both refugees and women (Pittaway & Pittaway, 2004). Over fifty percent of refugee populations are composed of women and girls, who are often deprived of the protective frameworks that familial structures, national governments, and community networks typically provide (Martin, 2004). Martin (2004) contends that within the home environments, family structures function as a primary source of protection, delivering care, guidance, and security. Nonetheless, during the process of displacement, families may become fragmented, leaving women and girls devoid of this crucial system of protection, heightening their vulnerability to threats such as exploitation, trafficking, and gender-based violence (Tadesse et al., 2024). Similarly, national governments, which are generally responsible for safeguarding citizens' rights and protections through legal frameworks, become inaccessible to refugees, who frequently lack the legal recognition or entitlements in host nations for local protections to be availed (Taran, 2001). This is also the case for community networks which typically provide solidarity, cultural connections, and informal support as they are disrupted in the course of displacement (Feller, 2006). Consequently, refugees may find themselves in unfamiliar settings without the social bonds and community support that otherwise might provide resources and aid in times of need. Refugees face these vulnerabilities in both virtual and physical realms (Pittaway & Pittaway, 2004). Failure to address these risks within the legal framework of data protection directly undermines women's safety and security.

Refugee women, in particular, bear a disproportionate burden due to their dual status as refuges and as women, leading

to heightened risks of exploitation (Martin, 2004). Allen (2003) emphasizes that in contexts governed by patriarchal structures, where women's autonomy is severely limited, their personal data is often controlled or manipulated by male relatives, partners or state actors. Such control over their data exacerbates privacy violations leaving them vulnerable to exploitation (Allen, 2003). Moreover, in conflict zones or refugee camps, where women's movements and choices are often restricted, their digital footprints can be used as a tool of control, leaving them at risk of violence or trafficking when their data is exploited for malicious purposes (Simko, 2022). According to UN Women (2018) women's freedoms in Sudan have been historically restricted especially under regimes with stringent social laws.

Furthermore, research indicates that young women, including refugees between the ages of eighteen and twenty-four face disproportionately high levels of severe online harassment, with twenty-six percent reporting experiences of stalking (Duggan, 2023). The absence of specific legal frameworks for refugee data not only places these women at risk of exploitation but also exposes them to greater dangers (McSherry & Kneebone, 2008). A notable instance of this exploitation directed at refugee women includes reports indicating that traffickers utilize Facebook to orchestrate the sale of refugee women, including minors, for as little as several thousand euros (Cliver, 2014). This phenomenon was particularly pronounced in cases involving Syrian refugees, where human traffickers exploited social media platforms, exemplified by a page entitled 'Syrians up for marriage', to advertise refugee women to men from Gulf nations. In one documented case, the page garnered thousands of followers within a mere five days and was only terminated following extensive protests from human rights advocates (Cliver, 2014).

Refugee women's dependency often forces them to rely on male relatives or humanitarian aid for access to essential resources, including technology (Liebig & Tronstad, 2018). This dependency limits their ability to independently access and use

digital tools and platforms, as they may lack the financial means or decision-making power to obtain devices, secure internet connections, or even maintain privacy in their online activities (UNHCR, 2018). This lack of autonomy can make them vulnerable to having their digital interactions monitored or controlled by male family members, further restricting their freedom and access to information (Bauloz et al., 2019). Additionally, refugee women who are economically dependent are less likely to have the resources or support systems to protect themselves from such threats (Henshaw, 2023). For example, they may lack the financial independence to change devices, upgrade security measures, or access legal support if they encounter online harassment. This combination of economic dependency and exposure to gender-based violence creates a digital environment where refugee women are particularly vulnerable, as they are both restricted in their ability to engage freely online and at higher risk of exploitation and abuse (Henshaw, 2023).

Language and cultural barriers further isolate refugees and these factors make it difficult for refugees to effectively engage with digital tools and services that require literacy and technical skills. This isolation not only limits their ability to access vital services but also increases their susceptibility to digital exploitation (UNESCO, 2023). Without the ability to communicate effectively, refugees are less likely to understand privacy policies or recognize potential threats to their data, leaving them more exposed than their male counterparts (Pierik, 2022).

These obstacles, coupled with the prevalence of online gender-based violence (OGBV), leave refugee women uniquely vulnerable to privacy violations and digital exploitation (Zotti, 2023). OGBV manifests through cyberstalking, harassment, and non-consensual sharing of intimate images, often targeting refugee women who lack support systems and legal protections.

Notwithstanding, there is no extant primary legislation tackling this peril in Sudan. The only significant effort so far is the Sudanese Cybercrime Law of 2007 (the Cybercrime Act)—

however, this law is insufficient. The Cybercrime Act contains provisions related to data privacy, but it lacks specific protections for refugees, and this leaves a significant legal gap that disproportionately affects refugee women (Data Protection Africa, 2022). Section 2 of the Cybercrime Act extends the scope of the law to offenses committed 'wholly or in part in or outside Sudan' (Data Protection Africa, 2022). While this provision aims to cover cybercrimes affecting Sudanese systems or individuals across borders, it fails to account for the transnational nature of data handling specific to refugee populations (Salah et al., 2019). Section 8 of the Cybercrime Act stipulates that an individual who accesses an information system and intentionally destroys or deletes data shall face a prison sentence not exceeding six years, a fine, or both penalties. However, the Act does not clarify whether its provisions extend to refugees, whose data is frequently managed by international organizations and host nations as they traverse borders (Henshaw, 2023). This deficiency is critical given the unique adversities faced by refugees (Kilic et al., 2019).

The absence of specific legal safeguards engenders a significant vulnerability for refugees, who lack explicit recourse should their data be exploited beyond Sudan's jurisdiction. This legal inadequacy is particularly concerning in light of the biometric data collection practices that are frequently integral to refugee registration procedures. For instance, the United Nations High Commissioner for Refugees (UNHCR) operates a Biometric Information Management System (BIMS) in Sudan for the purpose of registering refugees. While BIMS has demonstrated effectiveness in the identification of refugees, it has raised notable privacy concerns, as sensitive data may be subject to misuse if not sufficiently protected (Larter, 2023). For refugees, these privacy risks are amplified, as inadequate safeguard of such personal data could lead to tracking, harassment, profiling, and discrimination (Kilic et al., 2019).

It is upon this backdrop that this paper advocates for immediate legislation on the protection of refugees' privacy rights in

Sudan. This study employs a qualitative literature review methodology, drawing on both primary sources, such as legislative documents and reports from humanitarian organizations, and secondary sources, including academic research on data protection, and refugee rights. This paper is structured as follows: Part I is the introduction and provides the context and justification for focusing on refugees in Sudan, especially refugee women, emphasizing the unique risks they face in the absence of comprehensive data protection laws. Part II discusses the imperative of privacy rights and highlights the plight of refugees as a result of their status. Part III provides an analysis of the data protection risks that refugees in Sudan face as a result of a lack of a principal data protection legislation and special data protection body. Part IV highlights some of the legislative gaps in protecting the privacy rights of refugees in Sudan. In Part V, the paper makes a few recommendations and concludes.

II. THE RIGHT TO PRIVACY AND DATA PROTECTION FOR REFUGEES

Over two-point five quintillion (million trillion) bytes of data are collected worldwide every day (Karjian, 2024). This unprecedented scale of data collection amplifies the need for robust data protection frameworks, given that a significant portion of this data includes sensitive and personal information. While data is a powerful and valuable resource, capable of driving innovation and enhancing lives, its misuse can have devastating consequences for both individuals and organizations (Karjian, 2024).

In the context of refugees, particularly in Sudan, the importance of data protection cannot be overstated. Refugees are among the most vulnerable populations globally, often subject to discrimination, exploitation, and systemic marginalization (Warso, 2013). Data protection is essential for ensuring the dignity, safety, and security of refugees. Sensitive information such as biometric data, health records, and personal histories is

routinely collected during registration processes and by humanitarian organizations. Without proper safeguards, this data can be exploited for harmful purposes, including discrimination or tracking by malicious actors (Warso, 2013).

Data protection is important for various reasons. It helps uphold the fundamental right to privacy, shielding individuals from unwarranted surveillance or misuse of their information (Fuster, 2014). Effective safeguards prevent sensitive data from being weaponized for trafficking, identity theft, or other exploitative practices (Rodatá, 2009). When refugees trust that their data is being handled securely, they are more likely to engage with aid organizations and participate in essential services including education and healthcare. Proper data governance empowers refugees, particularly women, by giving them autonomy over their personal information and ensuring equitable access to digital tools and resources (Fuster, 2014).

The right to privacy entails an individual having full protection in person and in property as proposed and argued by Rubenfeld (1989). This right is a fundamental human right that guarantees individuals the freedom from unwarranted intrusion into their personal life (Griffin, 2007). It allows people to protect their personal information, communication, family life, home, and correspondence (Warso, 2013).

The right to privacy is one of the rights most widely demanded today (Reis et al., 2024; McCloskey, 1980). The current demand for privacy arises from two main factors. Firstly, the increased affluence of people in prosperous societies during the twentieth century has made privacy more accessible and desirable for the majority. Second, advancements in invasive technology now pose a significant threat to this newfound privacy (McCloskey, 1980).

The right to privacy is protected by various international and regional human rights instruments. These instruments include: the Universal Declaration of Human Rights (UDHR) (a. 12); the

International Covenant on Civil and Political Rights (ICCPR) (a. 17); the African Charter on Human and Peoples' Rights (ACPR) (a. 5); and the African Union Convention on Cyber Security and Personal Data Protection that was adopted on 27th June 2014 is a significant legal framework that addresses aspects related to cybersecurity and personal data.

Privacy is a fundamental right that is essential for every individual. Its significance is amplified for marginalized populations who are often overlooked in privacy and security matters (Tabassum & Faklaris, 2024). Refugee women represent one of the most vulnerable and marginalized groups in the world. They must deal with a complex web of gender discrimination and numerous human rights violations (Rathore & Yadav, 2023).

Refugees fleeing war and persecution are in a vulnerable position because their country of origin does not afford them protections; indeed, often it is their own governments that are persecuting them. Once they cross the border into another country, they have fewer rights as non-citizens in the host country, which leaves them vulnerable to abuse. While the UNHCR and several non-governmental organizations (NGOs) have a mandate to protect refugees, the laws related to their protection are rarely enforced, in some regions, they are non-existent. Refugees also cannot rely on protection from law enforcement and legal mechanisms in host countries that protect citizens, because many law enforcement agencies are specifically tasked with finding, detaining, or deporting them (Purkey 2013). This also means that, without equal access to mechanisms that enforce data protection laws, refugees are particularly vulnerable to violations of their rights.

During migration and registration, refugees leave behind traces of their personal data, including sensitive data about their identity, location, and personal history (Broeders, 2009). The registration of refugees consists of a series of activities including identification, recording of data, documentation, verification, case processing, and data management and exchange (Schoe-

maker et al., 2021). It is a continuous process that involves collection, storage, updating, and management of data (Bohlin, 2008). Refugees' data, including their identity, location, and personal history, constitute sensitive data, and, if mishandled, can expose them to risks such as exploitation, discrimination, and further violence (Williams, 2020). More particularly, as migration rates rise, the security and privacy of this data have become crucial concerns (Georgiou et al., 2023).

Another critical issue that arises in this context is the illusion of informed consent. Humanitarian organizations, responsible for delivering essential resources, often require the collection of extensive personal data to effectively administer aid (Beigbeder, 2023). This data collection includes not only identity verification but also sensitive information on health, family status, and financial resources, which are crucial for resource distribution (Hiedemann, 2024). Nonetheless, without comprehensive data protection protocols, refugees may be rendered vulnerable to exploitation, identity theft, and security threats (Hayes, 2017). While humanitarian organizations may seek consent from refugees before collecting their personal data this process is complicated by the inherent power imbalance between the two parties. Gazi (2020) argues that while consent is typically a legal basis for data collection, it may be impractical in refugee settings, where access to aid and services may be conditioned on the provision of data. According to Callamard (2002), this imbalance creates an environment where the refugees' ability to make autonomous decisions is compromised.

Refugees often rely on aid and services provided by these organizations, which can pressure them to comply with data requests even if they are uncomfortable doing so. Likewise, the aids and services are often urgent needs, hence, leaving little to no time for the data subjects to comprehend the risks at stake. Mulumba (2005) points out that the dependence on humanitarian aid can make the act of consenting feel coerced. When women need food, shelter, or medical care, refusing to give their per-

sonal information might seem impossible, especially if they fear losing access to these critical resources. In such situations, the refugees may not be able to provide 'freely given' consent due to the power imbalance created by their vulnerable status. Similarly, Gazi (2020) also argues that humanitarian organizations often process data to protect the vital interests of refugees, such as ensuring their safety and providing essential services like healthcare, food, and shelter. In such cases, the consent given may be involuntary and a façade, a product of the circumstances the refugees find themselves (Callamard, 2002).

This issue becomes even more complex when refugees lack access to the information necessary to make informed decisions. Language barriers and limited education may also prevent them from fully understanding what they are consenting to, as noted by Pittaway & Bartolomei (2003). The plurality of language is naturally expected in a setting comprised of a large population of less educated people who emanate from diverse backgrounds and have been forced to converge by life threatening circumstances. Without clear explanations of how their data will be processed and the potential long-term risks associated by sharing the data, refugees may ignorantly consent to data processing that could harm them in the future. Bohmer & Shuman (2017) further emphasize that in such settings, the concept of consent becomes more elusive. In countries like Sudan, where refugees face extreme vulnerabilities, they may not feel empowered to refuse or withdraw their consent without fearing negative repercussions (Mackenzie et al, 2007). This therefore undermines the core principle of informed consent, which should be based on voluntary, well-informed decision-making, free from any form of pressure or coercion (Hugman et al., 2011).

At this juncture, an essential question arises regarding safeguarding data privacy among refugee populations. That is, whether the imperative of data privacy takes precedence over fundamental and pressing livelihood needs, such as access to food, shelter, healthcare, and employment? As Gough and Gough

(2019) emphasize, refugees face multifaceted challenges that extend beyond digital concerns to encompass core survival requirements. Given the complexities of their circumstances, prioritizing data protection may initially appear secondary to pressing needs like securing adequate housing, legal recognition, and humanitarian assistance (Hiedemann, 2024). However, Hathaway (1997) argues that without adequate data safeguards, the collection of personal information exposes refugees to heightened risks, thus, highlighting how intertwined privacy concerns are with immediate survival.

Indeed, data privacy and livelihood needs may be profoundly interdependent (Hanrahan, 2015). Protecting refugees' personal data transcends mere digital security; it directly influences their capacity to access essential resources safely (Maitland, 2018). Improper management of refugee data can lead to discrimination, trafficking, or financial exploitation, all of which severely undermine efforts toward establishing stable livelihoods (Jacobsen, 2005). Thus, data privacy can be viewed as a crucial component of refugee well-being, creating a safer pathway to vital resources without the risk of privacy breaches or harmful consequences (Witteborn, 2021). This interdependence shows that data privacy and livelihood needs should not be conceptualized as competing priorities, but rather as synergistic dimensions of refugee protection (Jaspars & O'Callaghan, 2010), where each reinforces the other in fostering a secure and dignified existence for refugees.

In addressing the issue of data protection for refugees, it is essential to consider the broader legal frameworks that govern personal data protection. One of the most prominent frameworks in this regard is the European Union's General Data Protection Regulation ('the GDPR'), which, while does not specifically target refugee women or refugees in Sudan, provides significant protections for all individuals, including refugees, particularly regarding sensitive personal data. The GDPR offers heightened protection for certain categories of personal data, such as biomet-

ric data or information revealing racial or ethnic origin, which is often relevant to refugees, including refugees, who may face increased risks of exploitation or discrimination (Guggenmos et al, 2020).

Under the GDPR, processing sensitive data is strictly regulated and the legislation has specific provisions outlining when such data can be legally processed. This regulation requires that organizations processing such data must justify the necessity of the data collection by relying on one of several legal bases (Jasserand, 2024). In the context of humanitarian action, Gazi (2020) highlights the need for NGOs in humanitarian settings adhere to these legal bases when handling refugee data.

The GDPR emphasizes the need for informed consent in data processing, though obtaining 'freely given' consent in refugee settings may often be challenging due to the coercive dynamics at play. Humanitarian aid organizations must balance their operational needs with the necessity to respect the rights of refugees, which can be particularly difficult when data is collected as a prerequisite for receiving essential services. As Gazi (2020) explains, humanitarian organizations should consider alternative legal bases such as vital and legitimate interests when processing data to protect refugees' well-being and safety, especially in emergency situations.

In contrast, countries with weak or non-existent data protection laws, refugees are at a huge risk of their right to privacy being compromised (Alexander, 1999). For example, refugees are particularly vulnerable to the misuse of their personal information in regions such as Sudan, which lacks a comprehensive data protection framework (Suliman, 2019). Without clear legal safeguards, humanitarian actors, organizations and governments may collect and share sensitive data, including biometric and health information, without adequate oversight or protections (Holloway et al., 2022). This not only puts refugees at risk of identity theft, discrimination, and exploitation but also raises significant concerns about their privacy and autonomy (Lintner,

2024). It is therefore important for the country to formulate a national data protection law and a dedicated data protection body.

When refugees trust that their data is protected, they are more likely to engage with institutions and participate in programs designed to assist them (Doná, 2007). Data protection enables refugees to safely access financial services such as banking and microfinance (Bhagat & Roderick, 2020). Likewise, with secure data practices, refugees can participate in digital economies, including online education, e-commerce, and remote work (Easton & Hackl, 2023).

The empowerment of refugees is a vital component of data protection (Martin, 2004). Martin (2004) argues that by educating refugees about their data rights and equipping them with the means to control their personal information, these women can make informed decisions and protect themselves in the digital world. Therefore, within the context of this paper, it is essential that the law, particularly data protection laws, address the privacy challenges faced by refugees in Sudan.

III. CHALLENGES PLAGUING REFUGEE DATA PROTECTION IN SUDAN

Refugees in Sudan face unique and significant challenges regarding data protection, which directly impact their safety, security, and dignity (Akram, 2013). Privacy and security concerns are particularly significant for refugees who face unique risks such as discrimination, exploitation and physical harm when their personal information is exposed (Lingel et al., 2014). The collection of data from refugees by humanitarian organizations involves data and privacy-related risks as their data may be subjected to security breaches, leaks, hacks, inadvertent disclosure of their information, and discrimination (Vannini, 2020). The collection and potential misuse of their data poses significant risks, particularly for vulnerable populations like refugees, who

face unique threats to their safety and well-being if their data is not adequately protected (Tabassum & Faklaris, 2024). This paper discusses some of these challenges further.

A. Humanitarian organizations related risks

Humanitarian organizations are pivotal in providing humanitarian assistance for vulnerable populations and those deprived of their human rights (Vannini, 2020). As Vannini (2020) rightly highlights, these organizations rely heavily on data to carry out their missions effectively. However, this dependence on data collection and sharing poses significant risks, especially to sensitive populations like refugees in Sudan. Humanitarian organizations must handle sensitive and personal data with the utmost care to avoid risks of exploitation, trafficking and identity theft. The right to privacy especially in the context of refugees, includes ensuring that data is not misused for malicious purposes (Fuster, 2014).

The collection and sharing of data by humanitarian organizations is, in most cases, integral to their operations (Prakash et al., 2020). Humanitarian organizations share this data with their staff or members as well as implementing partners and affiliate organizations in the humanitarian sector (Williams, 2020). Their reliance on data sharing practices exposes refugees in Sudan to significant risks (Açıkyıldız, 2024).

One of the main concerns is the collection of biometric data in the form of facial recognition technology, fingerprints, and iris scans (Kaurin, 2019). The UNHCR (2024) has reported the registration of over 14,500 refugees in Sudan since January 2023, which involves gathering extensive personal information, including their biometric data. Martin (2004) argues that while this data is essential for providing aid and protection, its collection and use raise significant privacy concerns. The storage and sharing of such sensitive information create opportunities for data breaches and misuse, particularly in a region like Sudan, where

the civil war has severely compromised infrastructure, including civil documentation systems (UNHCR, 2024).

Moreover, the registration and documentation processes for refugees in Sudan encompasses data protection issues (Profile, 2024). Humanitarian organizations may not always have robust data protection measures in place. According to Williams (2020), the protection of personal data by humanitarian organizations is often insufficient and this leaves the data vulnerable to breaches and misuse by malicious actors. The risks are exacerbated when data is shared with other actors in the humanitarian space (Williams, 2020). A real-world example of such concerns came to light through the work of cybersecurity researcher Jeremiah Fowler, who discovered a non-password-protected database containing sensitive records such as scanned passports, ID Cards, victim stories including refugees related to the UN Trust Fund to End Violence against Women. This fund exposed one hundred and fifteen thousand records, including personal information of individuals and groups associated with the initiative. The unprotected database raised significant concerns about data privacy and the protection of vulnerable populations, and this illustrates the risks of inadequate cybersecurity and data management practices within global organizations (Fowler, 2024). This incident highlights the urgent need for more robust data protection measures, especially when handling sensitive information that can impact the safety and well-being of women and girls globally.

One of the key aspects of data protection as emphasized above is that refugees must be able to give free and informed consent for the collection and use of their data (Roth, 2009). The lack of bargaining power among refugee women complicates this issue. Lack of bargaining power leads to coerced consent. Refugee women's dependency on humanitarian aid places them in a coercive position where they may feel compelled to consent to data collection to access basic resources such as food, shelter or healthcare. This dynamic undermines the very principle of voluntary and informed consent as discussed above, as their consent is often influenced by

the power imbalances within refugee households and the urgent need for survival (Yingling, 2024). This lack of bargaining power makes it nearly impossible for refugees to exercise control over their personal data, thereby violating the core tenet of voluntary and informed consent (Yingling, 2024).

Refugee women, particularly in Sudan, often lack agency in their interactions with humanitarian organizations (Yingling, 2024). This lack of agency stems from a combination of socio-cultural, economic, and political factors that systematically disadvantage them. Refugee women in Sudan, as in many other conflict zones, are often dependent on male relatives for financial, social, and even legal support. This dependency extends to the provision of consent for engaging with humanitarian organizations (Amare et al., 2024). The process of giving consent for data collection in these settings is highly problematic.

Humanitarian organizations, in their efforts to streamline aid and services, often overlook the dynamics of power and control that exist within refugee households (Rathore & Yadav, 2023). In many cases, male relatives, who hold greater social and economic power within the family structure, are expected to act as gatekeepers for women's access to humanitarian assistance (Amare et al., 2024). This includes consenting to the collection of sensitive data, such as personal and biometric information. For refugee women, this situation can lead to a coerced or pressured form of consent (Deps et al., 2022). The refugee women may feel obliged to follow the wishes of their male relatives, even if they personally have reservations about sharing their data or engaging with the organization (Amare et al., 2024). This dynamic significantly undermines the voluntary nature of consent, as it is heavily influenced by familial hierarchies and social expectations, which may be further exacerbated in a context of conflict and displacement (Deps et al., 2022).

Yingling (2024) argues that the issue of bargaining power in this context reveals a critical gap in the protection of refugee women's rights, particularly their right to privacy and control

over their personal data. Refugee women, due to their limited social and economic power, are rarely able to negotiate the terms of their engagement with humanitarian organizations (Yingling, 2024). They do not have the agency to challenge the conditions under which their data is collected, shared, or stored. As a result, they are often unable to exercise full control over the consent process, which is fundamental to the ethical and legal handling of personal data (Ewers et al., 2021). In this environment, the consent process becomes not just a technical procedure, but a reflection of the broader power imbalances that exist within refugee communities (Mayer & Tran, 2022).

There is also often a lack of clear guidelines in some humanitarian organizations that provide migrant aid. This absence highlights an urgent need for the development and implementation of comprehensive data management protocols (Smith, 2022). This absence illustrates the need for developing and implementing comprehensive data management protocols to protect the sensitive information of vulnerable populations, such as refugee women in Sudan (Schoemaker et al., 2021). Humanitarian organizations should therefore develop and enforce protocols to ensure that sensitive data is handled with the utmost care and security (Kohli et al., 2023). This includes not only protecting the data itself but also ensuring that the consent of refugees is obtained in a manner that respects their autonomy and address the power dynamics at play.

The absence of clear protections for refugees' data facilitates the exploitation of their personal information by both domestic and international actors, particularly humanitarian organizations (Scarnecchia et al., 2017). These organizations, while providing aid directly or through affiliates, may prioritize their own commercial interests over the privacy rights of vulnerable populations. Addisalem (2024) highlights the potential for unaccountable private corporations to exploit refugee data, particularly in contexts where refugees have little or no control over their personal information.

Refugees in Sudan, already marginalized by their status as displaced persons, are disproportionately affected by these technological practices. The unregulated use of refugee data by both domestic and international actors contributes to a growing concern about privacy violations, further marginalizing refugees, especially refugee women, and perpetuating cycles of exploitation (Vaccaro & Madsen, 2009). Therefore, addressing the gap in data protection laws and integrating privacy protections into humanitarian practices in Sudan is crucial to safeguarding the dignity and rights of refugees (Scarneccia et al., 2017).

B. Lack of Data Protection Laws for refugees in Sudan

The absence of a comprehensive data protection law in Sudan significantly compromises the privacy and security of refugees (Abusharaf, 2009). In nations such as Kenya with robust data protection frameworks, such laws provide clear guidelines for the handling of personal data, including mechanisms for legal redress when these guidelines are breached. However, in Sudan, the lack of such a framework means that refugees have limited options for protecting their data privacy and seeking justice when their rights are violated (Kaurin, 2019). This legal vacuum exacerbates the vulnerabilities of refugee women, who are already among the most marginalized and at-risk populations (Memela & Maharaj, 2016). The absence of a legal structure leaves them exposed to the misuse of sensitive data, such as health records, identification documents, and personal histories, which can increase their susceptibility to exploitation and abuse.

The lack of a Data Protection Authority (DPA) in Sudan significantly hinders the enforcement of privacy laws, which are essential for ensuring the security of refugees' personal information (Hofmann & Mustert, 2023). Without a dedicated agency to enforce these laws, the risk of data misuse becomes significantly higher, with the absence of mechanisms for accountability and redress (Hartzdog & Solove, 2014). The absence of a DPA in Su-

dan exacerbates this issue by not only neglecting the need for tailored mechanisms to protect refugees but also failing to ensure fair and efficient asylum procedures for their identification, registration, and protection.

This lack of national data protection legislation and body is further compounded by Sudan's failure to implement effective international and regional frameworks designed to protect refugees' rights. Sudan is signatory to the 1951 Refugee Convention and its 1967 Protocol, which outline the rights of refugees and the responsibilities of states to protect them. However, the absence of a national legal framework undermines Sudan's obligations to these international treaties, particularly in safeguarding the personal data of refugees (Slom, 2024). This results in significant gaps in the protection mechanisms for refugees, leaving them vulnerable to privacy violations and exploitation.

It is necessary to create a DPA in Sudan to align the national legal system with international and regional obligations, including implementing data privacy protections for refugees. A robust regulatory body will provide the necessary oversight to safeguard refugees' personal data, ensuring that it is not misused or accessed without consent. Furthermore, the establishment of such an authority would help ensure the country's compliance with international treaties like the 1951 Refugee Convention and the 2019 Declaration on Principles of Freedom of Expression and Access to Information in Africa, enabling Sudan to better meet its legal obligations to protect the rights of refugees, including their right to privacy (Bryant, 2020).

IV. DATA PROTECTION REGULATION GAP IN SUDAN

According to Hurwitz (2009), states are primarily responsible for ensuring the protection of refugees within their borders. This responsibility is enshrined in the 1951 Refugee Convention. Article 7 of this Convention mandates that refugees must be ac-

corded the same treatment as aliens, ensuring non-discrimination and the protection of their rights, including their physical security and well-being (Jastram & Achiron, 2001). However, these protections, while important, are insufficient in addressing the specific vulnerabilities faced by refugees in Sudan, especially in relation to their privacy and personal data protection.

As De Brujin (2009) notes, protecting the physical security of refugees extends beyond ensuring their bodily safety as it encompasses the protection of their dignity and autonomy. While the 1951 Refugee Convention does not explicitly address privacy, it can be interpreted as part of the broader principle of human security, which seeks to protect individuals from harm in all its forms, including that which arises from the misuse of personal information. Howard-Hassmann (2012) argues that privacy is inextricably linked to personal dignity and autonomy, both of which are fundamental to human security. Rouvroy (2008) further reinforces this perspective by asserting that safeguarding privacy, especially data privacy, is a crucial component of physical security. Thus, the failure to protect refugees' data undermines their security and breaches their human rights.

This concern is particularly pertinent in Sudan as a country grappling with political instability and limited capacity to uphold its international obligations, including those related to refugee protection (Massoud, 2011). Sudan was suspended from the African Union in 2019 by the African Union Peace and Security Council and this situation has further complicated its ability to engage in meaningful legal reforms or implement international standards for refugee protection (ReliefWeb, 2024). In this context, the legal framework for refugee data protection in Sudan remains rudimentary at best. While Sudan is a signatory to the ACHPR, which enshrines the right to privacy under Article 12, the application of this right to refugees remains ambiguous and inadequately enforced (Massoud, 2011).

Sudan's history regarding data protection is marked by significant challenges, particularly in the context of political up-

heaval and the lack of a comprehensive legal framework. The former regime, led by Omar al-Bashir, employed extensive surveillance tactics to monitor citizens, utilizing imported technologies for privacy invasion (Suliman, 2019). This included tools from companies like Blue Coat Systems and Hacking Team, which allowed for interception of encrypted communications without proper judicial oversight (Suliman, 2019). Although there are laws that theoretically protect privacy, such as Article 74 of the 2018 Telecommunications and Postal Regulation Act, these are often circumvented. The vague definitions in laws like the Cybercrime Act and use of vague terms like 'competent authorities,' allows authorities to access personal data without a court order, undermining citizens' privacy rights (Hamad & CIPESA Writer, 2021).

Following the ousting of al-Bashir in 2019, Sudan adopted a new constitution that enshrines the right to privacy (Article 55) and free expression (Hamad & CIPESA Writer, 2021). However, the enforcement of these rights remains weak due to ongoing political instability and lack of effective governance (Suliman, 2019). There is no independent data protection authority in Sudan to oversee compliance with privacy laws. This absence allows both government entities and private companies to mishandle personal data without accountability (Hamad & CIPESA Writer, 2021).

To understand the depth of the legal gaps in Sudan, this highlights the existing sectoral laws. Article 55 of the Sudanese Constitution guarantees the right to privacy, including privacy of correspondence. Article 74 of the Telecommunications and Postal Regulation Act, 2018 allows for surveillance and interception of communications with judicial authorization but fails to account for the specific vulnerabilities of refugees. The Cybercrime Act, 2007 addresses unauthorized data access but offers no provisions on how to handle data pertaining to refugees, particularly women. Similarly, while Article 28 of the Electronic Transactions Act, 2007 criminalizes unauthorized access to encrypted

data, it does not provide clear protections for the personal data of refugees.

Sudan lacks a dedicated data protection law, leaving personal data vulnerable to misuse. Although laws like the Electronic Transactions Act, 2007, the Cybercrime Act, 2007, and the Telecommunications and Postal Regulation Act, 2018 provide some provisions on data privacy, these laws are focused primarily on cybersecurity and national security and not specifically on protecting refugees' data.

Furthermore, Sudan lacks a designated DPA to monitor or enforce data protection laws (Suliman, 2019). Suliman (2019) argues that institutional void leaves refugees' data particularly vulnerable, as there is no oversight on how personal data is collected, stored, or used during refugee registration and documentation processes. Without proper legal safeguards and enforcement mechanisms, the risk of discrimination, identity theft, and other human rights violations increases significantly (Mannion, 2020; Sapre & Singh, 2024).

In the context of Sudan, the absence of robust data protection laws creates a permissive environment for the imposition of foreign data practices by international organizations, which may disregard the privacy and security needs of refugees. This further entrenches existing power imbalances, leaving these women vulnerable to exploitation and privacy violations.

V. RECOMMENDATION AND CONCLUSION

A. Recommendations

To effectively address the digital vulnerabilities faced by refugees in Sudan, particularly concerning data privacy and protection, the following recommendations should be considered, focusing on practical implementation in a challenging environment like Sudan:

1. Data Protection Impact Assessment

A key recommendation emerging from this study is the mandatory implementation of DPIAs by organizations, including international agencies, NGOs, and governmental bodies, that collect or process the personal data of refugees in Sudan. To address the risks faced by refugees in Sudan, the implementation of DPIAs should be gradual and adapted to Sudan's context. Given Sudan's limited infrastructure and the political instability that the country is facing, a practical first step would be to pilot DPIAs within international agencies and local NGOs operating in the two main refugee camps, Um Rakuba and Tunaydbah in eastern Sudan. Given the technological challenge, these assessments can initially be conducted using paper based tools to identify and mitigate the data protection risks. The process should begin with mapping the types of sensitive data being collected, such as biometric information or personal identifiers, and assessing the associated risks such as privacy breaches, exploitation, identity theft, discrimination, harassment, and other privacy violations.

DPIAs should then focus on risk mitigation strategies that are feasible taking into account the resource-constrained circumstances. Some of the risk mitigation strategies may include utilizing low-technology encryption methods for storing sensitive data locally rather than transmitting the data over insecure channels. In addition, regular low-cost evaluations should be conducted to assess the effectiveness of implemented measures. Local community members, including refugees can be trained to serve as monitors for DPIA compliance, provide feedback and identify potential breaches.

i). Challenges In Implementing DPIAs

One of the major challenges likely to be faced in implementing DPIAs for refugees in Sudan is the limited infrastructure and technology available in refugee camps. Refugee camps often lack reliable internet access and necessary technical equipment

to conduct thorough data assessments (Nwankwo & Otieno, 2024). As explained by Hallinan & Martin (2020), for DPIAs to be more effective, there needs to be access to digital tools that can analyze and mitigate risks but for Sudan's current fragile infrastructure, such tools may be unavailable and there is a need to rethink the strategies that will be used to implement DPIAs in the camps. This paper suggests analogue methods.

Another significant obstacle is the absence of comprehensive data protection legislation in Sudan (Raymond et al., 2016). Without a proper legal framework, there is no local standard for humanitarian organizations to follow when conducting DPIAs (Massoud, 2011). These organizations are then forced to rely on private and international laws, which may not be all fitting to refugees in Sudan (Keller & Brennan, 2007). A lack of local legislation additionally means that there are no legal consequences for organizations that fail to adequately protect the data of refugees, further diminishing the effectiveness of DPIAs (Jay & Hamilton, 1999).

Cultural and gender barriers are another significant challenge humanitarian organizations are likely to face when it comes to implementing DPIAs in Sudan. According to Jaji (2015), refugees are often subjected to restrictive gender norms. As explained by LeRoux-Rutledge (2020), in many Sudanese refugee communities, there is a general expectation for women to prioritize domestic responsibilities, an aspect that prevents them from engaging in data protection training or participating in DPIA processes. The cultural barriers in place further contribute to a lack of awareness among refugees about their data rights and the risks associated with data misuse. This issue is further compounded by illiteracy, as many refugees in Sudan lack the educational background required to understand the technical aspects of data protection (Ossome, 2013). The sky-high illiteracy rates severely limit their ability to comprehend how their personal data is collected, used or shared, making it difficult for them to give informed consent or engage in DPIA-related discussions.

2. Legal Framework and Data Protection Authority (DPA)

The absence of comprehensive data protection laws in Sudan leaves refugees vulnerable to privacy violations. Establishing a robust legal framework is essential, but it must be a gradual process taking Sudan's extant political instability and resource limitations into account. A practical starting point would be to introduce basic data protection guidelines through existing legal mechanisms, such as amendments to existing laws governing refugees and vulnerable populations. These guidelines should focus on ensuring that sensitive data, particularly that of women, is protected from misuse and exploitation.

The establishment of a Data Protection Authority (DPA) should follow a phased approach. Initially, the DPA could function within an existing governmental body, such as the Ministry of Justice. This would reduce the need for extensive new infrastructure and provide a cost-effective solution for monitoring and enforcing data protection measures. The DPA's mandate should include offering guidance on data privacy practices, monitoring compliance with national and international standards, and addressing violations.

International partnerships could also play a crucial role in supporting the development of Sudan's data protection infrastructure. These partnerships could provide technical expertise and resources to draft legislation and establish regulatory bodies while helping build political support for data protection reforms.

3. Institutional accountability

Strengthening institutional accountability for data protection is important to ensure that organizations handling refugees' data adhere to ethical standards. A practical approach to this issue would involve introducing a mandatory self-reporting system, where organizations, including international agencies and NGOs, are required to publish and submit annual reports outlining their data handling practices. These reports should

detail how data is collected, stored, used, alongside the enacted measures to protect the privacy of refugees. These self-reports would then be reviewed by a temporary Data Protection Authority (DPA) or a similar body.

Finally, incentives for compliance with data protection standards should be introduced, such as offering certifications for organizations that consistently meet data protection criteria. Penalties for non-compliance could include restrictions on funding or operational activities, ensuring that institutions remain accountable to both legal frameworks and the communities they serve.

B. Conclusion

Refugees in Sudan are exposed to significant risks related to data protection, including identity theft, privacy breaches, and the exploitation of their personal information by humanitarian actors. These risks are heightened by their vulnerability due to displacement, gender-based violence, discrimination, and the lack of a comprehensive legal framework in Sudan to protect their data. In the absence of a comprehensive data protection law, humanitarian organizations often collect sensitive information, such as health records and biometric data, without adequate safeguards. This results in the infringement of refugees' privacy rights.

This paper highlights the importance of integrating DPIAs as a key strategy for mitigating these risks. DPIAs enable organizations to systematically identify, evaluate, and address the risks associated with processing refugees' data, ensuring that sensitive information is handled with a high degree of ethical and operational security. By implementing DPIAs, humanitarian organizations can develop robust, preventative data protection protocols, thus reducing the likelihood of breaches and unauthorized access.

Additionally, this paper advocates for the formulation of a data protection law and the establishment of a DPA in Sudan. Such developments would provide the legal and regulatory structure necessary to enforce data privacy standards, holding organizations accountable for the ethical handling of refugees' data. Given Sudan's current political and infrastructural limitations, these measures could be introduced gradually, beginning with pilot projects and collaborations with international stakeholders. Such an incremental approach allows Sudan to build the administrative and technical foundations for data protection.

REFERENCES

Abusharaf, R. M. (2009). *Transforming displaced women in Sudan: politics and the body in a squatter settlement*. University of Chicago Press.

Addisalem, A (2024). *The State of AI-Driven Humanitarian Big Data Governance and Law in Africa.*

African Union (2014). African Union Convention on Cyber Security and Personal Data Protection.

Akram, S. M. (2013). Millennium development goals and the protection of displaced and refugee women and girls. *Laws*, *2*(3), 283-313.

Alexander, M. (1999). Refugee status determination conducted by UNHCR. *International Journal of Refugee Law*, *11*(2), 251-289.

Allen, A. L. (2003). *Why privacy isn't everything: Feminist reflections on personal accountability*. Rowman & Littlefield.

Amare, S., Adamek, M. E., & Minaye, A. (2024). Barriers to accessing social support at refugee-serving humanitarian organizations. *Cogent Social Sciences*, *10*(1), 2342597.

Bauloz, C., Vathi, Z., & Acosta, D. (2019). Migration, inclusion and social cohesion: Challenges, recent developments and opportunities. *World Migration Report 2020*, 186-206.

Beigbeder, Y. (2023). *The role and status of international humanitarian volunteers and organizations: The right and duty to humanitarian assistance* (Vol. 12). BRILL.

Bhagat, A., & Roderick, L. (2020). Banking on refugees: Racialized expropriation in the fintech era. *Environment and Planning A: Economy and Space*, *52*(8), 1498-1515.

Bohlin, A. (2008). Protection at the cost of privacy? A study of the biometric registration of refugees.

Broeders, D. (2009). *Breaking down anonymity: Digital surveillance of irregular migrants in Germany and the Netherlands* (p. 230). Amsterdam University Press.

Bryant, J. (2020). Africa is in the information age: Challenges, opportunities, and strategies for data protection and digital rights. *Stanford Technology Law Review, 24,* 389.

Callamard, A. (2002). Refugee women: A gendered and political analysis of the refugee experience. In *Global changes in asylum regimes* (pp. 137-153). London: Palgrave Macmillan UK.

Cliver, M. (2014). *Human trafficking for sexual exploitation and networked technology: Mobile phones, social networking and he Internet* (Doctoral dissertation, New York University).

Constitution of Sudan, Article 55 (2019).

Data Protection Africa. (2022, May). Sudan Fact Sheet. Retrieved July 15, 2024, from Sudan Fact Sheet | Data Protection Africa.

Data Protection Africa. (2023, May). Africa: AU's Malabo Convention set to en-

ter force after nine years. Retrieved October 2, 2024, from Africa: AU's Malabo Convention set to enter force after nine years (dataprotection.africa).

Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019.

Deps, P. D., Rezende, I., Andrade, M. A., & Collin, S. M. (2022). Ethical issues in research with refugees. *Ethics, Medicine and Public Health*, *24*, 100813.

Doná, G. (2007). The microphysics of participation in refugee research. *Journal of Refugee Studies*, *20*(2), 210-229.

Duggan, M. (2023, October 22). Online Harassment. Pew Research Center. Retrieved November 9, 2024 from https://www.pewresearch.org/internet/2014/10/22/online- harassment/.

Easton-Calabria, E., & Hackl, A. (2023). Refugees in the digital economy: The future of work among the forcibly displaced. *Journal of Humanitarian Affairs*, *4*(3), 1-12.

Ewers, M. C., Gengler, J., & Shockley, B. (2021). Bargaining power: A framework for understanding varieties of migration experience. *International Migration Review*, *55*(4), 1121-1151.

Feller, E. (2006). Asylum, migration and refugee protection: realities, myths and the promise of things to come. *International Journal of Refugee Law*, *18*(3-4), 509-536.

Fowler, J. (2024, October 22). UN Trust Fund to End Violence against Women exposed in data breach. Retrieved December 13, 2024 from https://www.vpnmentor.com/news/report- unwomen-breach/

Fuster, G. G. (2014). The emergence of personal data protection as a fundamental right of the EU (Vol. 16). Springer Science & Business.

Gauci, J. P., Giuffré, M., & Tsourdi, E. L. (Eds.). (2015). *Exploring the boundaries of refugee law: Current protection challenges* (Vol. 3). Hotei Publishing.

Gazi, T. (2020). Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. *Journal of International Humanitarian Action*, *5*(1), 9.

Gehlen, R. G. S., Arboit, J., Paula, C. C. de, & Padoin, S. M. de M. (2020). Perspectives of knowledge about violence against migrant women: Mapping academic production Strictu Sensu. *Research, Society and Development,* (11), e99291110546.

Georgiou, T., Baillie, L., & Shah, R. (2023). Investigating concerns of security and privacy among Rohingya refugees in Malaysia. *arXiv preprint arXiv:2304.01617*.

Gilman, M., & Green, R. (2018). The surveillance gap: The harms of extreme privacy and data marginalization. *NYU Review of Law & Social Change*, *42*, 253.

Gough, H. A., & Gough, K. V. (2019). Disrupted becomings: The role of smartphones in Syrian refugees' physical and existential journeys. *Geoforum*, *105*, 89-98.

Griffin, J. (2007). The human right to privacy. *San Diego Law Rev*iew, *44*, 697.

Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., & Fridgen, G. (2020). How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: Evidence from the German asylum procedure.

Hallinan, D., & Martin, N. (2020). Fundamental rights, the normative keystone of DPIA. *European Data Protection Law Review*, *6*, 178.

Hamad, K., & CIPESA Writer. (2021, December 23). Sudan's bad laws, internet censorship and repressed civil liberties. *CIPESA*. Retrieved December, 13, 2024 from https://cipesa.org/2021/12/sudans-bad-laws-internet-censorship-and-repressed-civil- liberties/

Hanrahan, K. B. (2015). Living care-fully: The potential for an ethics of care in livelihoods approaches. *World Development*, *72*, 381-393.

Hathaway, J. C. (Ed.). (1997). *Reconceiving international refugee law* (Vol. 30). Martinus Nijhoff Publishers.

Hayes, B. (2017). Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and 'big data'. *International Review of the Red Cross*, *99*(904), 179-209.

Henshaw, A. (2023). Addressing the digital gender gap. In *Digital Frontiers in gender and security* (pp. 42-62). Bristol University Press.

Hiedemann, A. M. (2024). Navigating the humanitarian nexus: unveiling humanitarian supply chains, aid to assistance shifts, and AI synergies in international organizations.

Hofmann, H. C., & Mustert, L. (2023). Data protection. In *Research Handbook on the Enforcement of EU Law* (pp. 461-475). Edward Elgar Publishing.

Holloway, K., Al Masri, R., & Yahia, A. A. (2022). *Digital identity, biometrics and inclusion in humanitarian responses to refugee crises*. ODI.

Howard-Hassmann, R. E. (2012). Human security: ndermining human rights? *Human ights Quarterly*, *34*(1), 88-112.

Hugman, R., Bartolomei, L., & Pittaway, E. (2011). Human agency and the meaning of informed consent: reflections on research with refugees. *Journal of Refugee Studies*, *24*(4), 655-671.

Human Rights Watch. (2017). Sudan: Refugee women at risk of GBV and exploitation.

Hurwitz, A. G. (2009). *The collective responsibility of states to protect refugees*. OUP Oxford.

ILO. (2024, July). Partnership for improving prospects for forcibly displaced persons and host communities.

Jacobsen, K. (2005). *The economic life of refugees*. Kumarian Press.

Jaji, R. (2015). Normative, agitated, and rebellious femininities among East and Central African refugee women. *Gender, Place & Culture, 22*(4), 494-509.

Jasserand, C. 15. (2024) Biometric data, within and beyond data protection. *The Boundaries of Data*, 295.

Jastram, K., & Achiron, M. (2001). *Refugee protection: guide to international refugee law*. Geneva: IPU/United Nations High Commissioner for Refugees

(UNHCR).

Jay, R., & Hamilton, A. (1999). Data protection. *Law and Practice*, *2*.

Kaurin, D. (2019). Data protection and digital agency for refugees.

Keller, E. M., & Brennan, P. K. (2007). Cultural considerations and challenges to service delivery for Sudanese victims of domestic violence: Insights from service providers and actors in the criminal justice system. *International Review of Victimology*, *14*(1), 115 141.

Kenya Data Protection Act, 2019.

Kohli, N., Aiken, E., & Blumenstock, J. (2023). Privacy guarantees for personal mobility data in humanitarian response. *arXiv preprint arXiv:2306.09471*.

Larter, T. L. (2023). Concerns of power and policy in the use of biometrics by UNHCR.

LeRoux-Rutledge, E. (2020). Re-evaluating the 'traditional': How the South Sudanese use established gender narratives to advance women's equality and empowerment. *World Development*, *132*, 104929.

Liebig, T., & Tronstad, K. R. (2018). Triple disadvantage?: A first overview of the integration of refugee women.

Lingel, J., Naaman, M., & Boyd, D. M. (2014, February). City, self, network: Transnational migrants and online identity work. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 1502-1510).

Lintner, C. (2024). 'They must know their rights'–Reflecting on privacy, informed consent and the digital agency of asylum seekers and refugees in border contexts. *International Migration*, *62*(5), 71-87.

Mackenzie, C., McDowell, C., & Pittaway, E. (2007). Beyond 'do no harm': The challenge of constructing ethical relationships in refugee research. *Journal of Refugee Studies*, *20*(2), 299-319.

Maitland, C. (Ed.). (2018). *Digital lifeline?: ICTs for refugees and displaced persons*. MIT Press.

Mannion, C. (2020). Data imperialism: The GDPR's disastrous impact on Africa's e- commerce markets. *Vanderbilt Journal of Transnational Law, 53(*2), Article 6.

Martin, S. F. (2004). *Refugee women*. Lexington books.

Massoud, M. F. (2011). Do victims of war need international law? Human rights education programs in authoritarian Sudan. *Law & Society Review*, *45*(1), 1-32.

Mayer, T., & Tran, T. (Eds.). (2022). *Displacement, belonging, and migrant agency in the face of power*. Abingdon: Routledge.

McCloskey, H. J. (1980). Privacy and the right to privacy. *Philosophy*, *55*(211), 17-38.

McSherry, B., & Kneebone, S. (2008). Trafficking in women and forced migration: Moving victims across the border of crime into the domain of human rights. *International Journal of Human Rights*, *12*(1), 67-87.

Memela, S., & Maharaj, B. (2016). Challenges facing refugee women. A critical review. *Global Change and Human Mobility*, 53-72.

Mulumba, D. (2005). *Gender relations, livelihood security and reproductive health among women refugees in Uganda. The case of Sudanese women in Rhino Camp and Kiryandongo Refugee Settlements*. Wageningen University and Research.

Nwankwo, I., & Otieno, N. (2024). Adopting data protection impact assessment (DPIA) in Africa: Lessons from Kenya's DPIA framework and experiences. In *African Data Protection Laws* (pp. 77-110). De Gruyter.

OCHA (2024). Sudan - Humanitarian Data Exchange (humdata.org).

Office of the Data Protection Commissioner (2024) Data Commissioner Urges Humanitarian Organizations to Prioritize Dignity of Data Subjects at Privacy Symposium Conference 2024 - Office of the Data Protection Commissioner (ODPC) Retrieved on October 3, 2024.

Ong, L. M., & Findlay, M. (2023). A realist's account of AI for SDGs: Power, inequality and AI in community. In *The Ethics of Artificial Intelligence for the Sustainable Development Goals* (pp. 43-64). Cham: Springer International Publishing.

Organization of African Unity (OAU), *African Charter on Human and Peoples' Rights ('Banjul Charter')*, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), 27 June 1981.

Ossome, M. A. R. I. L. Y. N. (2013). Abduction, confinement and sexual violence against south Sudanese women and girls in Kakuma refugee camp, Kenya. *After the Comprehensive Peace Agreement in Sudan*, 158-175.

Pierik, B. (2022). Patriarchal power as a conceptual tool for gender history. *Rethinking History,* 26(1), 71-92.

Pittaway, E. and Bartolomei, L. (2003) Women at risk field research report: Thailand 2003. Sydney, Centre for Refugee Research, University of New South Wales.

Pittaway, E., & Pittaway, E. (2004). 'Refugee Woman': A dangerous label: Opening a discussion on the role of identity and intersectional oppression in the failure of the international refugee protection regime for refugee women. *Australian Journal of Human Rights*, *10*(1), 119-135.

Prakash, C., Besiou, M., Charan, P., & Gupta, S. (2020). Organization theory in humanitarian operations: A review and suggested research agenda. *Journal of Humanitarian Logistics and Supply Chain Management*, *10*(2), 261-284.

Profile, C., & Jones, M. (2024). Refugees/Migrants.

Rathore, P., & Yadav, H. (2023). A comparative analysis of human rights for refugee women: Challenges, progress, and implications for policy and advocacy. *DME Journal of Law*, *4*(02), 29-39.

Raymond, N., Al Achkar, Z., Verhulst, S., Berens, J., Barajas, L., & Easton, M. (2016). Building data responsibility into humanitarian action. *OCHA Policy and Studies Series*.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27

April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Reidenberg, J. R. (2002). Privacy wrongs in search of remedies. *Hastings Law Journal*, *54*, 877.

Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). Privacy law challenges in the digital age: A global review of legislation an enforcement. *International Journal of Applied Research in Social Sciences*, *6*(1), 73 88.

Rodotà, S. (2009). Data protection as a fundamental right. In *Reinventing data protection?* (pp. 77-82). Dordrecht: Springer Netherlands.

Rouvroy, A. (2008). Privacy, data protection, and the unprecedented challenges of ambient intelligence. *Studies in Ethics, Law and Technology*, *2*(1).

Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review*, 737-807.

Salah, A. A., Pentland, A., Lepri, B., & Letouzé, E. (2019). Guide to mobile data analytics in refugee scenarios. *The 'Data for Refugees Challenge' study*. Cham: Springer.

Sapre, A., & Singh, S (2024). Between war and peace: Exploring the role of refugee law in the context of Sudan political conflict. *International Migration*. https://doi.org/10.1111/imig.13278.

Scarnecchia, D. P., Raymond, N. A., Greenwood, F., Howarth, C., & Poole, D. N. (2017). A rights-based approach to information in humanitarian assistance. *PLoS currents*, *9*.

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2021). Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development*, *27*(1), 13-36.

Simko, L. (2022). *Humans and vulnerability during times of change: Computer security needs, practices, challenges, and opportunities*. University of Washington.

Slom, F. A. A. (2024). The role of good governance in promoting human rights in Sudan. *American Journal of Arts and Human Science*, *3*(3), 15-22.

Smith, N., Idris, M. Y., Schüür, F., & Ko, R. (2022). Data for good, what is it good for? Challenges, opportunities, and data innovation in service of refugees.

Sudan Cybercrime Act, (2007).

Sudan Electronic Transactions Act, Article 28 (2007).

Sudan suspended from the African Union - Sudan. (2024, June 21). ReliefWeb. https://reliefweb.int/report/sudan/sudan-suspended-african-union.

Sudan Telecommunications and Postal Regulation Act , Article 74 (2018).

Suliman, M. (2019, November). The right to privacy in Sudan: A call to enact a data protection act. [Web]. Retrieved July 15, 2024 from https://advox.globalvoices.org/2019/11/05/the-right-to-privacy-in-sudan-a-call-to- enact-a-data-protection-act/.

Tabassum, S., & Faklaris, C. (2024). Digital privacy for migrants: Exploring current research trends and future prospects. *arXiv preprint arXiv:2406.02520*.

Tadesse, G., Andualem, F., Rtbey, G., Nakie, G., Takelle, G. M., Molla, & Tinsae, T. (2024). Gender-based violence and its determinants among refugees and internally displaced women in Africa: Systematic review and meta-analysis. *BMC Public Health*, *24*(1), 2851.

Taran, P. A. (2001). Human rights of migrants: Challenges of the new decade. *International Migration*, *38*(6), 7-51.

The African Charter on Human and Peoples' Rights, (1981).

UN (1951). Convention Relating to the Status of Refugees, Article 1 (A) (2).

UN General Assembly, International Covenant on Civil and Political Rights, United Nations, Treaty Series, vol. 999, p. 171.

UN General Assembly, Universal Declaration of Human Rights, 217 A (III).

UN High Commissioner for Refugees (UNHCR), Implementation of the 1951 Convention and the 1967 Protocol Relating to the Status of Refugees, EC/SCP/54, 7 July 1989.

UN Women. (2018). Assessment of Sudan women's movement (1980-2018). Retrieved December 13, 2024 from state_of_the_womens_movement_in_sudan.pdf.

UN Women. (2024). A year of suffering for Sudanese women and girls. Retrieved December 13, 2024 from https://sudan.un.org/en/265952-un-women-year-suffering-sudanese- women-and-girls.

UNESCO. (2023). *Key data on girls and women's right to education.* https://www.unesco.org/en/articles/key-data-girls-and-womens-right-education

UNFPA. (2018). *Gender Justice & the Law: Sudan*. https://arabstates.unfpa.org/en/publications/gender-justice-law-sudan.

UNHCR (2018, March 7). *Her Turn: UNHCR report reveals critical gap in education for refugee girls* [Press release]. https://www.unhcr.org/news/news-releases/her-turn- unhcr-report-reveals-critical-gap-education-refugee-girls.

UNHCR (2018). Registration and Identity management. Retrieved December 13, 2024 from https://www.unhcr.org/registration-guidance/.

UNHCR (2018). UNHCR Strategy on Digital Identity and Inclusion. https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/05/2018-02-Digital- Identity_02.pdf#:~:text=Tags.

UNHCR (2020). *The impact of forced displacement and statelessness in 2020—Trends, crises and responses*. https://www.unhcr.org/wp-content/uploads/sites/27/2022/06/UNHCR- global-trends-report_2020.pdf.

UNHCR. (2023) UNHCR's Biometric Tools in 2023. Retrieved December 13, 2024 from https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/.

UNHCR. (2023). *Gender-based violence*. (Global Report 2023*)*. https://reporting.unhcr.org/global-report-2023/outcome-areas/gender-based-violence.

UNHCR. (2024). Protection brief: Sudan. [Report].

UNHR. (2022, October 19). *Privacy and data protection: Increasingly precious asset in digital era says UN expert*. [Press release]. https://www.ohchr.org/en/press- releases/2022/10/privacy-and-data-protection-increasingly-precious-asset-digital-era- says-un.

Vannini, S., Gomez, R., & Newell, B. C. (2020). 'Mind the five': Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations. *Journal of the Association for Information Science and Technology*, *71*(8), 927-938.

Warso, Z. (2013). There's more to it than data protection–Fundamental rights, privacy and the personal/household exemption in the digital age. *Computer Law & Security Review*, *29*(5), 491-500.

Williams, O. (2020). *The Interface of Information Security, Risk, and Privacy on the Humanitarian Frontline*. American University.

Witteborn, S. (2021*).* Data privacy and displacement: A cultural approach. *Journal of Refugee Studies, 34*(2), 2291-2307.

World Food Programme. (2023). Unequal access: Gendered barriers to humanitarian assistance. Retrieved December 13, 2024 from https://www.wfp.org/publications/unequal-access-gendered-barriers-humanitarian- assistance.

World Health Organization. (2021). Introducing the WHO technical package on quality of care in fragile, conflict-affected, and vulnerable settings. Retrieved July 12, 2024 from https://www.who.int/news/item/24-03-2021-introducing-the-who-technical- package-on-quality-of-care-in-fragile-conflict-affected-and-vulnerable-settings.

World Health Organization. (2024). Sudan conflict and refugee crisis, Multi-country External Situation Report #1 – 18 June 2024. Retrieved December 13, 2024, from https://www.who.int/publications/m/item/sudan-conflict-and-refugee-crisis-1.

Yingling, J. (2024). Intersecting influences: Exploring intimate partner violence among Sudanese refugees in the Great Plains.

Zotti, S. S. (2023). Online violence: A gender-based phenomenon.