UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE E STUDI INTERNAZIONALI

Corso di laurea *Magistrale* in European and Global Studies

Legal Frameworks to Combat Non-Consensual Pornography on the Internet

Comparing the remedies afforded by EU's General Data Protection Regulation, Brazil's Lei Geral de Proteção de Dados, copyright law and technology.

Relatore: Prof. GUIDO GORGONI

Laureanda: Raquel Minuzzi Wild
Matricola N. 2041148

A.A. 2023/2024

To those who survived and their unwavering belief in justice, to those who lent credence to their words, and to those who fight tirelessly for a safer and fairer world.

Agradecimentos | Acknowledgements

Esta tese começou muito antes de eu sequer colocar a caneta no papel, muito antes de orientações e contagens de palavras ditarem meu caminho, porém, ela jamais existiria sem Deus ao meu lado. Ele forneceu a força. Ele plantou a semente deste sonho em meu coração, e Ele tornou tudo possível. Toda a honra e glória são atribuídas a Ele, cuja bondade me envolveu, concedendo-me amor e oportunidades além dos meus sonhos mais profundos.

À minha família, Fabiane, Fernando, Pedro, Débora e Ariane. Eu não estaria aqui sem todo o suporte, compreensão e amor que me mandaram do outro lado do oceano.

Mãezinha, palavras não seriam suficientes para agradecer o quanto você acreditou em mim, investiu nos meus sonhos e manteve seus braços abertos caso algum dia eu precisasse de alento. O seu amor me constrange e me torna todos os dias uma pessoa melhor. Obrigada por me mostrar todos os dias que a vida é bonita e as pessoas podem ser boas.

Pai, pelos seus sacrifícios e exemplos, eu agradeço publicamente. Por compartilhar literaturas, por me levar para faculdade de direito e plantar uma sementinha de busca por justiça desde que era um pingo de gente. Obrigada por acreditar que eu era extraordinária antes mesmo de eu sequer saber o significado disso.

Pedro, você acreditou nos meus sonhos quando eu não acreditei. Sua fé em mim fortaleceu a minha própria, e por isso, sou infinitamente grata. Apesar de prometer inúmeras vezes te escrever um reconhecimento público, me vejo sem palavras — porque seria incapaz de expressar o quanto sou grata pela sua existência. Obrigado por ser meu irmão, meu amigo e minha inspiração.

Débora, esta jornada foi possível apenas porque mantive nossas lembranças, momentos e um amor incondicional tingido de saudade em meu coração. Se estou aqui hoje, é porque você uma vez me pediu para ficar. Obrigado por ser meu ponto de apoio e minha melhor amiga.

Dra. Helena, Dra. Dani, Dra. Maria e Dr. Pedro, meus mais sinceros agradecimentos por serem minha torcida, por vibrarem e comemorarem cada uma das minhas conquistas. Por terem acreditado em mim e serem exemplos de profissionalismo, muito obrigada.

To my supervisor, your kindness, empathy, knowledge, and patience will forever be etched in my memory. Professors and supervisors like you make students like me, from small towns with big dreams, believe that the world is much larger and interesting when you're armed with knowledge. Grazie per todo.

Luisa, Elisa, and Gaia, sharing life with you was a gift beyond my wildest dreams. You cried, laughed, talked and supported me through every moment of doubt. I wouldn't be here without you. I struggle to find words to express my gratitude in English, Italian, Portuguese, or Luisiano, but I hope you understand how much I cherish the family we've created in Padova.

To the friends I made along the way, from Cascavel, to Padova and Tallinn: Thank you. For lending an ear to my stories, reading my work, guiding me back to myself, and believing in me when I felt alone. Life is better with you.

To myself, who dared to believe in a dream, who weathered the storm and found resilience amidst chaos: You did it. You survived and found in these words a strength that you thought was lost. To the little girl who dared to dream, my footsteps now echo around the world because you once believed in something greater than your hometown: thank you.

To all the women that talked about Non-Consensual Pornography, to those who were brave enough for fighting for themselves, to those who fought for other women, that listened to their stories and believed in their words: Thank you.

To Catarina and her siblings, I hope one day you read all of this and feel proud. This was for you, and the better world that I hope you get the chance to live in.

Raquel Minuzzi Wild / Legal Frameworks to Combat Non-Consensual Pornography: Comparing the remedies afforded by EU's General Data Protection Regulation, Brazil's *Lei Geral de Proteção de Dados,* copyright law and technology.

Chapter 1
Introduction

Non-Consensual Pornography is another modern form of gender violence against women that is spreading fast through nations and countries and increasing the need of legal instruments to protect the victims and avoid this kind of exposition. For instance, here are a few examples that cover this issue:

Anna was 16 when her ex-boyfriend send a video of an intimate moment to his friends at school. Melissa was 24 when her boyfriend drugged, filmed and threatened her with the images of her rape. Hackers gained unauthorized access to Carolina's personal computer, where they found private and intimate photographs. Subsequently, the hackers demanded a ransom in exchange for not releasing the compromising images. When she refused to pay the ransom, the hackers went ahead and posted the explicit photos online.

Lauren was scrolling down on her social media feed when she saw a topless picture of her in a random profile using her name, and gaining followers every day as they post her explicit pictures without her consent in their account. After getting a restraint order against her ex-husband, Susanne discovered that her private pictures were posted on a website alongside her full name and personal information.

In 1888, Le Grange Brown, a professional photographer based in New York, was accused of selling pictures of "undraped women" in local salons. The problem is that those weren't real, he took pictures of high society young girls, cut and pasted their heads to images of explicitly naked women. Now in the contemporary epoch characterized by the swift intertwining of digital connectivity, where interpersonal bonds are forged with a mere click.

Those are not isolated cases, nor rare in the daily lives of women all around the world. When we talk about data nowadays, we're speaking of a valuable product that can be trade, sell, used and interpreted for different purposes. But when we speak about Non-Consensual Pornography, we are also talking about intimacy, trust, trauma,

prejudiced behaviors and more than anything, we're talking about a modern kind of gender violence.

In this research, we aim to address the existent regulations that should safeguard the victims, how they might be failing during the processes and which other legal instruments could be used to protect the privacy, the data and the personality of the victims.

1.1 Background

When it comes to the modern society and the women's bodies, it was always felt and sold like a product, talking about the selling of altered pictures of women[1] or the exploration of their images, online or not. However, when the internet became a part of daily life for most, Non-Consensual Pornography started to scare and threaten the intimacy and freedom of women all over the world. Websites like IsAnyoneUp.com[2] or MyEx.com[3] were created with the main goal of exposing not only full names, addresses and other personal and sensitive data, they were essentially created to post videos and pictures of intimate moments filmed, created and spread without consent. Those websites were shut down one by one, but, not surprisingly, others were appearing with the same goal — revenge.

Most of those contents were uploaded to the website after blackmailing episodes, relationships breakups and disappointment with the female ex-partners. That's how the term "Revenge Porn" appeared, but nowadays, after understanding the guilt and victim blaming behind this expression, the Non-Consensual Pornography term is more acceptable and appropriate for those cases. It's also important to say that those websites were highly profitable for the owners that asked for money in order to remove those contents online, but not only that, they could actually make money with this exposition because people had genuine interest in this kind of pornography. On the article[4] wrote by one of the most important papers of the planets, this business was

[1] Remembering the case mentioned in the previous section where a professional photographer, was accused of selling pictures of "undraped women" in local salons.

[2] The pornographic website was shut down on the 19th of April 2012.

[3] The FTC shut down the Non-Consensual Pornography website on the 9th of January 2018.

[4] "Why We Find Hunter Moore And His 'Identity Porn' Site, IsAnyoneUp, So Fascinating" published by Forbes on the 5th of April 2012, available here:

considered a complete success because it turned a porn website into a “phone book” because you could have access not only to the pictures but also their address, Facebook page and even their personal phone number — What today is considered absurd, in that time, was a simple way to capitalize on social networking.

The escalating popularity and attention surrounding cybercrimes of this nature have raised alarm bells, extending concerns far beyond the mere security of internet data. These multifaceted issues not only underscore the immediate personal toll on victims but also shine a spotlight on a more pervasive societal ill: the glaring absence of adequate legislation and regulations to effectively combat the insidious nature of gender-based violence in the cyber realm.

That’s when and how Data Protection laws were created around the world. The global nature of the problem emphasizes the imperative of fostering a united front, where nations collaborate in enacting effective legislation and policies as a robust deterrent against the malicious dissemination of non-consensual intimate images. In essence, the discourse surrounding Non-Consensual Pornography has transcended its initial localized origins, morphing into a critical global dialogue that demands sustained and collective action — it is important to understand that the nations around the world have some kind of consensus recognizing that Non-Consensual Pornography is a crime that should be punished one way or another. However, the legislations may vary as they can be specific in some places (e.g. Germany, The United Kingdom and others) or broader in others (Japan, Canada and The Philippines, for example). In order to safeguard the dignity and well-being of women. In the intricate web of conversations surrounding Non-Consensual Pornography and cybercrime, the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados, or LGPD) emerge as distinct yet converging forces, each shaping the global response to the pervasive challenges of privacy violations in the digital age.

The GDPR, implemented by the European Union in May 2018, serves as a comprehensive framework aimed at fortifying and unifying data protection for individuals within its jurisdiction. Its principles, rooted in upholding individual rights

---

https://www.forbes.com/sites/kashmirhill/2012/04/05/hunter-moore-of-isanyoneup-wouldnt-mind-making-some-money-off-of-a-suicide/

and stringent data processing regulations, have global resonance. On the other side of the globe, the LGPD, enacted in September 2020 in Brazil, mirrors the GDPR's commitment to safeguarding personal data, tailored to the Brazilian context. Both regulations emphasize the paramount importance of explicit consent in processing personal data, providing individuals with a robust mechanism to control how their information is handled. In the context of Non-Consensual Pornography, both the GDPR and the LGPD recognize the violation of privacy and offer avenues for affected individuals to seek legal redress. These legal frameworks stand as beacons against the malicious dissemination of intimate images, offering victims a pathway to reclaim control over their personal data.

1.2 Research Objective

The main objective of this research is to identify the similarities and differences between regulations applied in Europe and Brazil, showing also the context of creation of the relevant laws and the context of application. Also, during the confection and data collection for this research, we came across contents and initiatives made mostly by women and victims to protect and find other resources for those who are facing the same issues they already had to. More than anything, this study has as an objective to be an instrument of information and data gathering in order to find eventual solutions and remedies in Brazil or in the countries where the GDPR is applied.

In this digital age and with the plurality of application of laws and instruments, this research also has a purpose of identifying what could be the extra legal tools to stop the spreading of Non-Consensual Pornography in social media platforms or websites that might be created specially for that.

Ideally, this thesis aims to become a comprehensive resource that provides victims with a sense of support, understanding, and empowerment. It should serve as more than just a scholarly study; rather, it should offer a safe haven and a source of reassurance for individuals grappling with the challenges of Non-Consensual Pornography. Within these pages, victims should find not only an analysis of the issue at hand but also practical guidance on how to navigate their circumstances, protect themselves from harm, and seek redress for the violations they have endured.

1.3 Relevance of the Study

When it comes to the reasons of the relevance and the interest of this subject, the answer can be either simple or complex. In the ever-evolving landscape of our digital age, a distressing trend has emerged—a new form of gender violence that exploits the vast reach of the internet to inflict harm, sow destruction, and shamelessly expose women. It's disheartening to witness this insidious practice gaining traction, morphing into a concerning societal phenomenon. What was once hailed as a platform for connection and empowerment is now being cynically weaponized to target and victimize women, marking a disturbing shift in the dynamics of gender-based violence.

The use of the internet as a tool for subjugation and humiliation is escalating, underscoring the urgent need to confront the complex challenges posed by this troubling trend. As technology advances, the ways in which abuse can be perpetrated, creating an environment where harm against women is not only facilitated but, distressingly, normalized. The virtual space, which should be a haven for equality and inclusivity, is increasingly tainted by the shadow of gender violence, as individuals exploit its anonymity to launch campaigns of degradation against women without consequence.

This unsettling evolution serves as a stark reminder of the immediate need for comprehensive measures to combat online gender violence. Our efforts must extend beyond traditional legal frameworks, reaching into the digital realm to ensure that the internet remains a platform for positive discourse and empowerment, rather than a breeding ground for harm. It's crucial to cultivate collective awareness and mobilize resources to dismantle the structures that allow such online abuses to proliferate. Only through a united and sustained commitment to eradicating this new and insidious trend can society hope to protect the well-being and dignity of women in the digital age.

The continual emergence of cutting-edge tools poses a growing challenge in establishing clear boundaries on how and when technology should be deployed to ensure the protection of individuals from online harm. The dynamic nature of technological advancements outpaces the formulation of adequate safeguards, demanding an ongoing and adaptive dialogue among legislators and advocates to effectively counter the ever-evolving landscape of digital threats.

In navigating these intricate dynamics, it becomes evident that legal and regulatory frameworks must evolve in harmony with technological advancements to provide robust protection against the diverse dimensions of online harm. A proactive approach is essential, one that not only recognizes existing legislative gaps but actively seeks to bridge them, ensuring the development of a more holistic and responsive legal infrastructure aligned with the evolving nature of digital challenges.

In delving into the multifaceted realm of effective policies, the research aims not merely to acknowledge their existence but to extract nuanced insights into their operational mechanisms. By scrutinizing policies that have exhibited notable success, the research seeks to unravel the intricate tapestry of strategies, methodologies, and underlying principles that contribute to their effectiveness. It aspires to move beyond a surface-level understanding and delve into the granular details, extracting lessons that transcend theoretical frameworks and resonate in the practical domain.

Simultaneously, a comprehensive comparative analysis with international counterparts forms an integral component of the research methodology. The global nature of the digital landscape demands a panoramic perspective that extends beyond borders and cultures. By juxtaposing successful policies from various countries, the research seeks to illuminate cross-cultural insights, recognizing the contextual nuances that either fortify their effectiveness or reveal potential shortcomings. This cross-cultural exploration serves not only to enrich the understanding of successful policies, but also to foster a global dialogue that acknowledges the diversity of challenges faced by women in distinct socio-cultural contexts.

The prevalence of Non-Consensual Pornography in the digital age necessitates a profound understanding of its impact on individuals and society. As such, the relevance of the study lies in its potential to contribute actionable insights and strategies to mitigate the harmful consequences of this specific type of cybercrime. By exploring the existent laws, such as the GDPR, LGPD, Brazilian Civil Code, the copyright legislations in a comparative way, the study aims to build upon a foundation of knowledge, identifying gaps, and highlighting areas where interventions and remedies can be most effective to pave the way towards an online environment that is not only

safer but also conducive to the growth and empowerment of girls in the digital age and in the future.

1.4 Overview of scientific literature on possible remedies for Non-Consensual Pornography

The discourse surrounding the scourge of Non-Consensual Pornography in Brazil initially manifested in 2013, triggered by the tragic suicides of two underage girls from disparate regions of the country. These heart-wrenching incidents acted as a poignant catalyst, thrusting into the spotlight the profound and devastating consequences that the exposure to non-consensual intimate images can inflict upon individuals. This disturbing revelation prompted impassioned discussions among feminist groups and ignited debates within the hallowed halls of the Brazilian Congress, where policymakers grappled with the urgent need for legislative action.

A more nuanced exploration into the roots of this problem unveils a complex tapestry woven by the enduring legacy of patriarchal norms. The historical control exerted over women's bodies and the perpetuation of a celibate image have cast a long shadow, contributing significantly to the challenges faced by victims. Deeply ingrained societal constructs, which unjustly portray victims as culpable, propel some individuals to contemplate drastic measures such as forced displacement or, tragically, suicide.

However, the nuances in their application and enforcement reflect the distinct legal landscapes of the European Union and Brazil. The General Data Protection Regulation’s impact extends globally, as its principles influence international data protection discussions. First, the GDPR is a pioneer when it comes to privacy protection due to the historical context intertwined to the creation of this law. In 1948 the UN published the Universal Declaration of Human Rights (UDHR)[5], in its 12th article, they mentioned the right to privacy and the attacks against the honor of individuals. This was the first inspiration to the creation of the GDPR and other privacy laws around the world. But where data protection comes? After the 108 convention, open for signature in 1981, the members of the European Council entered a consensus that this convention didn’t approach all the relevant aspects of privacy and data protection, so they had to

[5] Available in: https://www.un.org/en/about-us/universal-declaration-of-human-rights

make a directive (95/46/EC, 1995)[6], that was used as regulation until the General Data Protection Regulation (GDPR)[7] repealed it.

It was not until 2018 that Brazil introduced the Lei Geral de Proteção de Dados (LGPD), a comprehensive data protection law with specific provisions tailored to domestic contexts and nuances. This legislation delineates the parameters and obligations governing the collection, processing, and management of data by both entities and individuals. It represents a significant milestone in shaping the framework within which companies and individuals in Brazil are mandated to handle data responsibly and uphold their respective duties in safeguarding personal information.

In essence, the GDPR and LGPD, while rooted in distinct legal contexts, stand united in their pursuit of individual data protection and privacy rights. As tools against cybercrime they act regulating how to track data and also how people should be responsible for eventual or intended leaks of it, they reflect a consensus that transcends borders when data is being seen as a product of the digital age, weaving a shared narrative of empowerment, accountability, and resilience in the face of the evolving challenges posed by the digital landscape.

[6] Available in: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[7] Available in: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1702761840360

Chapter 2
Non-Consensual Pornography and Personal Data Protection

2.1 Defining and Understanding Non-Consensual Pornography

Non-Consensual Pornography, commonly known as "revenge porn," has become an increasingly prevalent issue in the last decade, exacerbated by the ease with which individuals can distribute and publicize compromising images online. While this phenomenon is not confined to the digital realm, the internet's pervasive influence has magnified the problem, demanding urgent attention. A recent study revealed a disconcerting statistic: one in 25 online Americans has either fallen victim to having sensitive images posted without consent or has faced threats of such exposure.[8]

The Cyber Civil Rights Initiative (CCRI) and other advocacy organizations have responded to this alarming trend by lobbying for enhanced legal protections. Their efforts are mirrored by the experiences of public figures like Jennifer Lawrence, who has openly discussed the profound emotional trauma resulting from the unauthorized dissemination of private, intimate photos. Acknowledging the severity of the issue, 38 states have taken legislative action in the form of Non-Consensual Pornography laws, with a notable surge in such enactments occurring in recent years[9]. However, despite these strides, the efficacy of current legal safeguards remains incomplete, and comprehensive federal intervention has yet to materialize.

Beyond the legal landscape, it is imperative to recognize that the challenge posed by Non-Consensual Pornography extends beyond statutory frameworks—it is fundamentally a cultural issue with sociological implications that are inadequately explored. The under-theorization of these implications underscores the need for theoretical work to inform the optimal construction and implementation of criminal statutes. Furthermore, such theoretical endeavors have the potential to catalyze transformative changes in societal attitudes and behaviors.

---

[8] Amanda Lenhart et al., “Online Harassment, Digital Abuse, and Cyberstalking in America,” *Data & Society*, November 21, 2016, https://datasociety.net/library/online-harassment-digital-abuse-cyberstalking/.

[9] PJ Patella-Rey (2018) Beyond privacy: bodily integrity as an alternative framework for understanding Non-Consensual Pornography, Information, Communication & Society, 21:5, 786-791, DOI: 10.1080/1369118X.2018.1428653

A critical avenue for exploration is delving into the narratives and descriptions of harm provided by victims. By conducting in-depth research into the experiences of those affected, we can gain a nuanced understanding of the multifaceted impact of Non-Consensual Pornography. This deeper comprehension, in turn, can inform the development of more targeted and effective strategies to combat the issue.

Shifting focus to sexting, the creation and sharing of one's own sexual images have witnessed a surge in prevalence over the last decade, as documented by various studies[10]. When undertaken voluntarily and consensually, sexting serves positive functions, fostering intimacy, contributing to wellbeing, and facilitating the exploration of sexual identity[11]. However, when sexual content is shared unwillingly or coerced under threats, it can lead to adverse consequences, including heightened discomfort, symptoms of depression, anxiety, and even suicidal ideation and attempts. Such forced or unwanted scenarios related to sexting are collectively termed image‑based sexual abuse, encompassing non-consensual distribution, posting, or threats involving nude or sexual images, commonly photographs or videos[12].

Within the realm of image‑based sexual abuse, distinctive forms include sextortion and non-consensual sexting. Sextortion involves threatening to distribute sexual images to coerce the victim into compliance, even if the exposure of the images never materializes[13]. This form of abuse can evolve from images initially sent voluntarily by the creator, later weaponized to manipulate the victim into providing

---

[10] Yara Barrense-Dias et al., "Sexting and the Definition Issue," *Journal of Adolescent Health* 61, no. 5 (2017): 544–54, doi:10.1016/j.jadohealth.2017.05.009, Manuel Gámez-Guadix and Estibaliz Mateos-Pérez, "Longitudinal and Reciprocal Relationships between Sexting, Online Sexual Solicitations, and Cyberbullying among Minors," *Computers in Human Behavior* 94 (2019): 70–76, doi:10.1016/j.chb.2019.01.004. Mara Morelli et al., "Sexting, Psychological Distress and Dating Violence among Adolescents and Young Adults," *Psicothema*, 2016, https://redined.educacion.gob.es/xmlui/handle/11162/118365, Cristian Molla-Esparza, Emelina López-González, and Josep-María Losilla, "Sexting Prevalence and Socio-Demographic Correlates in Spanish Secondary School Students," *Sexuality Research and Social Policy* 18, no. 1 (2021): 97–111, doi:10.1007/s13178-020-00434-0.

[11] Nicola Döring and M. Rohangis Mohseni, "Are Online Sexual Activities and Sexting Good for Adults' Sexual Well-Being? Results From a National Online Survey," *International Journal of Sexual Health* 30, no. 3 (July 3, 2018): 250–63, doi:10.1080/19317611.2018.1491921, Laura Graham Holmes et al., "A Sex-Positive Mixed Methods Approach to Sexting Experiences among College Students," *Computers in Human Behavior* 115 (2021): 106619, doi:10.1016/j.chb.2020.106619, Sebastian Wachs et al., "How Are Consensual, Non-Consensual, and Pressured Sexting Linked to Depression and Self-Harm? The Moderating Effects of Demographic Variables," *International Journal of Environmental Research and Public Health* 18, no. 5 (March 5, 2021): 2597, doi:10.3390/ijerph18052597.

[12] Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence, & Abuse* 19, no. 2 (2018): 195–208, doi:10.1177/1524838016650189, Henry, Nicola, Asher Flynn, and Anastasia Powell. *Responding to'revenge Pornography': Prevalence, Nature and Impacts*. Criminology Research Grants Program, Australian Institute of Criminology, 2019.

[13] Janis Wolak et al., "Sextortion of Minors: Characteristics and Dynamics," *Journal of Adolescent Health* 62, no. 1 (2018): 72–79, doi:10.1016/j.jadohealth.2017.08.014.

more content, engaging in cybersex, or even coercing in-person sexual relations[14]. Incidents of sextortion, as described in a research[15], have been reported involving minors and young adults, with a concerning number feeling pressured to provide sexual images. Despite the gravity of such situations, a significant proportion of minors do not disclose these incidents, highlighting a critical gap in awareness and reporting.

Research on the prevalence of sextortion, particularly among adolescents, remains scarce. Some scholars[16] conducted an analysis among adolescents aged 12–17, revealing that 5% reported being victims of sextortion, while 3% admitted to perpetrating sextortion. Notably, both victimization and perpetration rates were higher for boys than for girls, and no significant age-related differences were found.

Another distressing facet of image‑based sexual abuse is non-consensual sexting. Revenge pornography can be defined[17] as the non-consensual sharing of explicit images motivated by revenge, whereas non-consensual sharing refers to distributing such content without the victim's consent, with motivations not always linked to revenge[18]. The term "revenge porn" may be misleading, as motivations can vary beyond revenge, including seeking social reinforcement, sexual gratification, or even perpetrating the act as a joke[19]. Highlighting the "non-consensual" nature of these images, rather than focusing on "revenge," is suggested to be more conceptually and terminologically accurate. Non-Consensual Pornography[20], centers on the distribution of sexually explicit images without the victim's permission, excluding instances of being pressured or coerced into sending such images (termed "pressured sexting"). Importantly, non-consensual sexting does not encompass the reception of unsolicited sexual content, which falls under the umbrella of "online sexual harassment" or

[14] Idem.

[15] Janis Wolak et al., "Sextortion of Minors: Characteristics and Dynamics," *Journal of Adolescent Health* 62, no. 1 (2018): 72–79, doi:10.1016/j.jadohealth.2017.08.014.

[16] Justin W. Patchin and Sameer Hinduja, "Sextortion Among Adolescents: Results From a National Survey of U.S. Youth," *Sexual Abuse* 32, no. 1 (2020): 30–54, doi:10.1177/1079063218800469.

[17] Kate Walker and Emma Sleath, "A Systematic Review of the Current Knowledge Regarding Revenge Pornography and Non-Consensual Sharing of Sexually Explicit Media," *Aggression and Violent Behavior* 36 (2017): 9–24, doi:10.1016/j.avb.2017.06.010.

[18] Idem.

[19] Henry, Nicola, Asher Flynn, and Anastasia Powell. *Responding to'revenge Pornography': Prevalence, Nature and Impacts*. Criminology Research Grants Program, Australian Institute of Criminology, 2019.

[20] Yanet Ruvalcaba and Asia A. Eaton, "Nonconsensual Pornography among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men.," *Psychology of Violence* 10, no. 1 (2020): 68–78, doi:10.1037/vio0000233.

"unwanted sexual attention"[21], distinct categories of technology-facilitated sexual violence.

Non-Consensual Pornography is a phenomenon reminiscent of sextortion, that is the intricate dynamics unfold when explicit sexual images, initially shared voluntarily within the confines of an intimate context like sexting, are later wielded and distributed by an aggressor for multifaceted motives. This nuanced behavior pattern has garnered attention in the realm of adult interactions, as evidenced by prevalent studies exploring the prevalence and ramifications of non-consensual sexting among this demographic[22]. However, the understanding of these occurrences among adolescents remains both limited and fragmented, prompting a crucial exploration into this domain.

Insights into adolescent non-consensual sexting behaviors have been gleaned from diverse studies that offer varying perspectives on the prevalence and manifestations of this digital phenomenon. Research conducted in 2019[23] gives as a significant contribution to the understanding of the phenomenon, revealing that approximately 11.1% of respondents had engaged in image-based sexual abuse behaviors since the age of 16, with a noteworthy gender disparity wherein a higher percentage was reported among male respondents compared to their female

[21] Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence, & Abuse* 19, no. 2 (2018): 195–208, doi:10.1177/1524838016650189 and Sebastian Wachs et al., "How Are Consensual, Non-Consensual. Pressured Sexting Linked to Depression and Self-Harm? The Moderating Effects of Demographic Variables," *International Journal of Environmental Research and Public Health* 18, no. 5 (March 5, 2021): 2597, doi:10.3390/ijerph18052597.

[22] Branch, Kathryn, Carly M. Hilinski-Rosick, Emily Johnson, and Gabriela Solano. "Revenge porn victimization of college students in the United States: An exploratory analysis." *International Journal of Cyber Criminology* 11, no. 1 (2017): 128-142, Manuel Gámez-Guadix et al., "Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults," *Sexuality Research and Social Policy* 12, no. 2 (2015): 145–54, doi:10.1007/s13178-015-0186-9, Nicola Henry and Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence, & Abuse* 19, no. 2 (2018): 195–208, doi:10.1177/1524838016650189.

[23] Anastasia Powell et al., "Image-Based Sexual Abuse: The Extent, Nature, and Predictors of Perpetration in a Community Sample of Australian Residents," *Computers in Human Behavior* 92 (2019): 393–402, doi:10.1016/j.chb.2018.11.009.

counterparts. Complementary studies[24] have enriched understanding by providing nuanced insights into adolescent non-consensual sexting.

Unearthed instances where university students had their intimate images, initially shared in a trusting environment, subsequently disseminated without their consent[25]. Other scholars[26] delved into the landscape of adolescent behaviors, revealing that 10% had engaged in the sending of explicit images of others. Another study also contributed[27] to this discourse by highlighting that 3% of adolescents reported the distribution or posting of their sexual images electronically without their explicit permission in the preceding month. In a related vein, scholars[28] added a layer of complexity by identifying that 4.5% of adolescents admitted to showing or forwarding sexually explicit images of someone to another person without due permission or, more alarmingly, posting such images on the internet. Intriguingly, age was identified as a factor influencing this behavior, with older adolescents more likely to engage in such actions, although no significant gender differences were found.

Synthesizing insights from multiple studies, a meta-analysis attempted to distill patterns in the prevalence of non-consensual sexting among adolescents. The meta-analysis revealed that 12.0% of adolescents had perpetrated non-consensual sexting, while 8.4% had experienced victimization. Notably, neither sex nor age emerged as significant determinants of perpetration or victimization. However, the meta-analysis underscores a critical gap, emphasizing the paucity of studies

---

[24] Heidi Strohmaier, Megan Murphy, and David DeMatteo, "Youth Sexting: Prevalence Rates, Driving Motivations, and the Deterrent Effect of Legal Consequences," *Sexuality Research and Social Policy* 11, no. 3 (2014): 245–55, doi:10.1007/s13178-014-0162-9

Kent Patrick et al., "Demographic and Behavioural Correlates of Six Sexting Behaviours among Australian Secondary School Students," *Sexual Health* 12, no. 6 (2015): 480, doi:10.1071/SH15004

Anne S. Frankel et al., "Sexting, Risk Behavior, and Mental Health in Adolescents: An Examination of 2015 Pennsylvania Youth Risk Behavior Survey Data," *Journal of School Health* 88, no. 3 (2018): 190–99, doi:10.1111/josh.12596

Joris Van Ouytsel, Michel Walrave, and Koen Ponnet, "An Exploratory Study of Sexting Behaviors Among Heterosexual and Sexual Minority Early Adolescents," *Journal of Adolescent Health* 65, no. 5 (2019): 621–26, doi:10.1016/j.jadohealth.2019.06.003.

[25] Strohmaier, Murphy, and DeMatteo, "Youth Sexting."

[26] Powell et al., "Image-Based Sexual Abuse."

[27] Patrick et al., "Demographic and Behavioural Correlates of Six Sexting Behaviours among Australian Secondary School Students."

[28] Van Ouytsel, Walrave, and Ponnet, "An Exploratory Study of Sexting Behaviors Among Heterosexual and Sexual Minority Early Adolescents."

contributing to a comprehensive understanding of this complex and evolving digital behavior.[29]

While strides have been made in understanding non-consensual sexting, challenges persist on the research frontier. A paramount necessity is the development of valid and reliable instruments to measure and comprehend the multifaceted dimensions of non-consensual sexting. Despite the wealth of information garnered from prior studies, the reliance on single-question methodologies highlights the need for more robust tools. These tools should not only possess psychometric properties but also demonstrate factor validity and concurrent validity concerning constructs such as depression, anxiety, and the broader spectrum of cyberbullying[30].

Compounding the challenges are inconclusive findings related to gender and age differences, contributing to the complexity of this evolving digital landscape. The need for a more nuanced understanding of the relationship between perpetration and victimization is evident, as existing studies have primarily focused on one aspect, leaving the interplay between these two dimensions insufficiently explored. A crucial gap in knowledge persists concerning adolescents, with limited information available compared to adults.[31]

Another critical limitation pertains to the lack of information on the temporal stability of image-based sexual abuse incidents. Unlike studies on other forms of cyberbullying that have demonstrated the stability of aggression and victimization over time, the temporal dynamics of non-consensual sexting remain unclear. Understanding whether these incidents are stable or sporadic phenomena is crucial for developing effective preventive and intervention strategies. Longitudinal studies could shed light on the stability of non-consensual sexting incidents over time and their potential impact on psychosocial adjustment among victims.[32]

---

[29] Sheri Madigan et al., "Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-Analysis," *JAMA Pediatrics* 172, no. 4 (April 1, 2018): 327, doi:10.1001/jamapediatrics.2017.5314.

[30] Vladlena Benson, *Handbook of Social Media Use Relationships, Security, Privacy, and Society. Volume 2* ([S.l.]: Academic Press, 2023).

[31] Manuel Gámez‐Guadix et al., "Assessing Image‐based Sexual Abuse: Measurement, Prevalence, and Temporal Stability of Sextortion and Nonconsensual Sexting ('Revenge Porn') among Adolescents," *Journal of Adolescence* 94, no. 5 (2022): 789–99, doi:10.1002/jad.12064.

[32] Idem.

In the context of contemporary discussions surrounding 'revenge porn,' a paradigm shift is proposed, urging a broader understanding of this phenomenon within the framework of a more comprehensive and nuanced concept – the 'continuum of image-based sexual abuse.' Revenge porn should not be isolated as an isolated, exceptional act; rather, it represents just one manifestation along a spectrum of gendered, sexualized forms of abuse that share common characteristics.[33]

By acknowledging the continuum of image-based sexual abuse and its alignment with broader forms of sexual violence, we argue for a more holistic perspective that better captures the multifaceted nature of the harms experienced by victim-survivors. This, we contend, lays the groundwork for the development of more effective educative and preventative strategies, aligning with the evolving landscape of digital interactions and power dynamics. This approach is not only grounded in theoretical underpinnings but draws on the collective expertise of scholars and researchers[34], providing a robust foundation for advancing both academic discourse and practical responses to combat image-based sexual abuse.

It is essential to emphasize that 'revenge porn' should not be considered in isolation as an exceptional act. Instead, it signifies merely one manifestation along a spectrum of gendered and sexualized forms of abuse that share common characteristics. By recognizing its place within a broader context of abusive behaviors, it can better understand the interconnectedness and underlying dynamics of such harmful actions.

The need for legislative and policy responses that mirror the nuanced nature of image-based sexual abuse is clear, acknowledging the continuum, and its alignment with broader sexual violence, may pave the way for more effective and targeted measures to address the root causes and consequences of these offenses. It is a firm belief that such a comprehensive strategy will not only better protect potential victims but also contribute to a cultural shift in attitudes and behaviors surrounding image-based sexual abuse.

---

[33] Clare McGlynn, Erika Rackley, and Ruth Houghton, “Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse,” *Feminist Legal Studies* 25, no. 1 (2017): 25–46, doi:10.1007/s10691-017-9343-2.

[34] Idem, Lynn Comella and Shira Tarrant, eds., *New Views on Pornography: Sexuality, Politics, and the Law* (Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC, 2015), Hampton, Jean. "Punishment, Feminism, and Political Identity: A Case Study in the Expressive Meaning of the Law." *Canadian Journal of Law & Jurisprudence* 11, no. 1 (1998): 23-45. doi:10.1017/S0841820900001673.

According to scholars[35], in the landscape of post-fordist capitalism, three pillars stand tall, shaping the contours of our current economic system: pornopower, pharmacopower, and the war industry. Each of these elements, according to scholars[36], significantly influences and determines the trajectory followed by our contemporary economic structures. In this intricate scenario, pornography emerges as more than mere adult content; it takes on the role of a sexual pedagogy, a mechanism intricately woven into the fabric of our society to produce certain truths. These truths, in turn, aim to exert control over subjectivities, acting as a formidable force through the realms of sexual and gender technologies.

Delving into the concept of sexual pedagogy sheds light on how these truths come to be, how they weave themselves into the very fabric of sexed bodies, and how they are performatively enacted in alignment with specific gender norms[37]. It is in this interrelation of power and knowledge that the differentiated construction of male and female sexualities plays a pivotal role.[38]

This differential construction contributes significantly to the pervasive objectification of the female body, a phenomenon that ripples through various forms of gendered violence. Nowhere is this more evident than in the realm of digital environments, where the contours of violence take on new shapes and dimensions. The unique socialization experiences of men and women play a role in perpetuating the dehumanization of the feminine, as representations of women as passive objects, submissive to male desires, strip them of their agency. Prevailing stereotypes, deeply rooted in societal consciousness, not only encourage chastity and modesty in women but also prescribe promiscuity as a criterion for assessing the value and virility of men.

Within our societal framework, a troubling tolerance, and at times an outright endorsement, exists for the violation—whether physical or metaphorical—of bodies

---

[35] Mariana Nascimento Maia and Rafael Baioni Do Nascimento, "Pornografia De Vingança No Ordenamento Jurídico-Penal Brasileiro," *Confluências | Revista Interdisciplinar de Sociologia e Direito* 24, no. 2 (August 1, 2022): 104–25, doi:10.22409/conflu.v24i2.53554.

[36] Paul B. Preciado, *Testo Junkie: Sex, Drugs, and Biopolitics in the Pharmacopornographic Era*, trans. Bruce Benderson (New York, NY: The Feminist Press at the City University of New York, 2013).

[37] Larissa Costa Duarte and Fabiola Rohden, "Entre o Obsceno e o Científico: Pornografia, Sexologia e a Materialidade Do Sexo," *Revista Estudos Feministas* 24, no. 3 (2016): 715–37, doi:10.1590/1806-9584-2016v24n3p715.

[38] Alexa Dodge, "Nudes Are Forever: Judicial Interpretations of Digital Technology's Impact on 'Revenge Porn,'" *Canadian Journal of Law and Society / Revue Canadienne Droit et Société* 34, no. 01 (2019): 121–43, doi:10.1017/cls.2019.4.

perceived as vulnerable and inherently feminine. Scholars[39] have delved into this disturbing facet, highlighting the underlying power structures and cultural norms that contribute to the perpetuation of such violence.

Unraveling the complex layers of gendered violence, it becomes evident that the delineation between virtuous women and prostitutes is deeply entrenched in societal perceptions of sex. The act of rape, in particular, becomes a stigmatizing force, tarnishing the victimized woman, while the moral judgment cast upon the man perpetrating the violation remains conspicuously absent[40].This stark double standard not only prevails, but also extends its influence into the realm of revenge porn.

Examining the societal response to revenge porn illuminates a dual moral lens that characterizes male and female sexualities in markedly different ways. The man, often viewed as virile and a conqueror, escapes the moral censure that is directed at the woman, who is labeled a prostitute and subjected to moral degradation. This pervasive double standard perpetuates harmful stereotypes, reinforcing gender inequalities within the broader context of sexual violence. [41]

In essence, the intersection of *pornopower*, gendered violence, and societal perceptions creates a complex tapestry that demands nuanced exploration. As we navigate this intricate landscape, it becomes imperative to dissect the cultural, social, and psychological dimensions that underpin the power dynamics shaping our understanding of sexuality and violence. Only through a comprehensive examination of these intersections can we hope to dismantle the entrenched structures that perpetuate gender inequalities and violence, paving the way for a more just and equitable society.[42]

---

[39] Lia Zanotta Machado, "Sexo, estupro e purificação", in Violência, Gênero e Crime no Distrito Federal, ed. Mireya Suárez e Lourdes Bandeira (Brasília DF: Paralelo 15: Editora Universidade de Brasília, 1999), 297-352.

Rita Laura Segato, "A estrutura de gênero e a injunção do estupro", in Mireya Suárez e Lourdes Bandeira (orgs.), *Violência, Gênero e Crime no Distrito Federal* (Brasília DF: Paralelo 15: Editora Universidade de Brasília, 1999), 387-427.

Lourdes Bandeira, "Violência sexual, imaginário de gênero e narcisismo", in Mireya Suárez e Lourdes Bandeira (orgs.), *Violência, Gênero e Crime no Distrito Federal* (Brasília DF: Paralelo 15: Editora Universidade de Brasília, 1999), 353-386.

Thomas Walter Laqueur, *Inventando o sexo: corpo e gênero dos gregos a Freud* (Rio de Janeiro: Relume-Dumará, 2001).

[40] Machado, "Sexo, estupro e purificação," *Violência, Gênero e Crime no Distrito Federal*, 297-352.

Anthony Giddens, *A Transformação da intimidade: sexualidade, amor e erotismo nas sociedades modernas*, traduzido por Magda Lopes (São Paulo: Editora da Universidade Estadual Paulista, 1993), 221.

[41] Dodge, "Nudes Are Forever."

[42] Nascimento Maia and Baioni Do Nascimento, "Pornografia de Vingança no Ordenamento Jurídico-Penal Brasileiro."

In reflecting on the distorted societal perceptions perpetuated by the double standards surrounding intimate content, our journey now ventures into a critical exploration of gender violence and its profound repercussions. The disparities in judgment between men and women caught on the web of intimate exposure pave the way for a deeper analysis of the broader implications of gendered violence. As we peel back the layers of this complex issue, the next section unveils the intricate connections between societal attitudes, power dynamics, and the lasting damage inflicted by gender violence.

2.2 Gender violence and its damages

The global concern surrounding gender violence, with its myriad dimensions, remains a critical focal point, emphasizing the intricate web of societal norms and power dynamics that perpetuate inequalities. In numerous cultures, the objectification of women as commodities further entrenches harmful practices, highlighting the challenges in dismantling deeply ingrained norms despite significant strides toward gender equality in the 21st century.

Brazil, in particular, serves as a stark example of the urgency and prevalence of gender violence, with a staggering statistic revealing that one in three women in the country falls victim to such acts.[43] This not only emphasizes the magnitude of the problem but also underscores the systemic nature of gender violence. What was once confined to the private sphere has rightfully emerged as a critical public health concern, recognizing that the impact of gender violence extends far beyond individual relationships, affecting the overall well-being of society.

Efforts to address gender violence in Brazil have led to the formulation of plans, agreements, and services. However, the persistent emergence of these efforts signals an ongoing battle, suggesting that existing measures may not be sufficiently comprehensive. The necessity for continued discussions about creating support networks reflects an awareness of the gaps in current response mechanisms. The objective extends beyond addressing the aftermath of gender violence to proactively

[43] FBSP – Fórum Brasileiro de Segurança Pública. *Visível e Invisível: A Vitimização de Mulheres no Brasil*. 4. ed. São Paulo: FBSP, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/03/visiveleinvisivel-2023-relatorio.pdf. Acesso em: 2 fev. 2024.

establishing structures that prevent it and provide necessary care and protection to those at risk or affected.

Turning our attention to Spanish legislation, which made significant legislative advancements[44] concerning the combat against gender violence, their unique and specific approach to gender-based violence serves as a microcosm of the global struggle against this pervasive issue. Moreover, Spain acknowledges that women experience violence not only within their families but also within their communities and by the state, pointing to a broader systemic issue. This multifaceted form of violence contributes to and is perpetuated by stereotypical ideas about the roles and expectations imposed on women. The differentiation of gender violence from domestic violence is clear on the legislation, specially on the Organic Act 1/2004 of 28 December on Integrated Protection Measures against Gender Violence, where they recognize domestic violence as something that occurs within the family, involving any family members and gender-based violence specifically targets women, involving acts of discrimination and power imbalance by a man towards a woman, even without cohabitation. It is a nuanced recognition of the varied contexts in which such violence manifests. The revelation that enduring relationships are often marked by violent situations serves as a stark reminder that gender violence permeates multiple layers of society.

Beyond the immediate physical harm, the psychological and societal implications deepen the roots of gender inequality. The recognition that the violence women face extends beyond their homes challenges societal norms, calling for a comprehensive reevaluation of existing structures and attitudes. Within this broader exploration, the psychosocial repercussions of the violation of privacy through the improper disclosure of intimate images become apparent. The experiences outlined in various documents shed light on the extensive damage inflicted upon women's lives, exposing a disturbing reality where victims not only endure immediate suffering but also grapple with enduring consequences, both psychologically and socially.

[44] These include Organic Act 11/2003 of 29 September, which addresses specific measures related to citizens' security, domestic violence, and the social integration of foreign nationals. Another significant development is Organic Act 15/2003 of 25 November, amending Organic Act 10/1995 of 23 November on the Criminal Code, and Act 27/2003 of 31 July, which regulates the Protection Order for Victims of Domestic Violence. Additionally, various Autonomous Communities have enacted laws within their jurisdiction, covering civil, criminal, social, and educational domains.

The disclosure of intimate images triggers a cascade of distressing events compromising various aspects of a woman's life. One document analyzed in a study[45] illustrates how an individual, after the end of a relationship, faced relentless pursuit, embarrassment, and threats in public spaces. The ex-partner's intrusive behavior extended to the workplace, negatively impacting the woman's professional life. Intimate photos and videos, improperly disseminated on the internet, subjected her to further humiliation, as colleagues were urged to view the content. This orchestrated campaign of psychological and reputational harm vividly demonstrates the deep and lasting impact of such actions.

Beyond the immediate aftermath of the violation, the social environment of victims becomes compromised, with friends commenting on the images and strangers making inappropriate remarks. The repercussions extend beyond mere annoyance, disrupting the victim's social life. Social isolation emerges as a significant consequence of the psychological and moral violence endured by women. Researchers point out that long-term psychic suffering damages self-esteem and social interaction, manifesting as post-traumatic stress, anxiety, and phobia.[46]

The consequences of gender violence can be exacerbated by guilt, shame, and embarrassment. Gender violence, as a public and complex problem, imposes restrictions on social life, leading to poor social acceptance, prejudice, and discrimination. In situations of violence, shame and social seclusion often result in isolation, reflecting the pervasive attitudes among women who have experienced such situations.

Moreover, the restriction of social interaction resulting from the dissemination of intimate images is not solely caused by men but is also perpetuated by women within the patriarchal structure. The power dynamics within relationships, shaped by patriarchal influences, underscore the control exerted over women's lives, especially within the sphere of sexuality.

---

[45] Manuel Gámez‐Guadix et al., "Assessing Image‐based Sexual Abuse: Measurement, Prevalence, and Temporal Stability of Sextortion and Nonconsensual Sexting ('Revenge Porn') among Adolescents," *Journal of Adolescence* 94, no. 5 (2022): 789–99, doi:10.1002/jad.12064.

[46] Cynthia Yoon et al., "Sexual and Physical Abuse and Identity of the Perpetrator: Associations with Binge Eating and Overeating in Project EAT 2018," *Eating Behaviors* 43 (2021): 101577, doi:10.1016/j.eatbeh.2021.101577.

In extreme cases, the violation of privacy can have severe consequences, as exemplified by the tragic suicide of a 16-year-old teenager[47]. The improper disclosure of her images led to unbearable suffering, highlighting the profound impact such violations can have on mental health and well-being.

In another case, Rose Leonel, after experiencing the release of intimate images, founded an NGO[48] aimed at providing legal, psychological, and digital expertise guidance for women in similar situations. Her personal account emphasizes the far-reaching consequences, including her children having to change schools due to classmates' comments and the compromise of her professional life.

The narratives in the documents underscore that psychological violence often precedes and follows the improper disclosure of intimate images. This form of violence compromises self-esteem, self-deprecation, and psychological health. The intensity and duration of suffering caused by such violations are evaluated by the judiciary, recognizing the challenge in quantifying and establishing a monetary value for the moral damage experienced by the women.

In different documents analyzed, the judges decided different values of indemnities for the victims ranging from R$ 7,880.00 to R$ 40,000.00, in attempt to address the moral damage and psychological suffering. The temporal gap between the release of images and the adjudication of compensation highlights the ongoing nature of psychosocial suffering.[49]

In essence, this type of violence is not only a threat to women's social lives but, more critically, to their very lives. The suffering and destabilization caused when women become aware of the disclosure underline the gravity of the issue. The pursuit of justice, as indicated by legal action, suggests an attempt to repair irreparable damage, acknowledging that the consequences may haunt victims throughout their lives.

---

[47] Available in: https://veja.abril.com.br/brasil/sexo-e-internet-quando-a-exposicao-pode-levar-a-morte

[48] The NGO founded by Rose Leonel is called Marias da Internet and aims to defend and orient victims of this type of crime in Brazil. Their Instagram account (https://www.instagram.com/mariasdainternet/) was created in 2017 when the founder went to a popular talk show in the country to launch this initiative, since then a series of fundraisings and events took place in order to raise funds and awareness.

[49] Carolina Scarpatto, Giovana Ilka Jacinto Salvaro, and Mônica Ovinski De Camargo, "Women in Situations of Violation of Privacy: Psychological and Moral Damage in the Context of Gender Violence," *Aletheia* 56, no. 1 (2023): 71–92, doi:10.4322/aletheia.005.en.

In the quiet corners of a woman's life, far beyond the tangible wounds and emotional bruises inflicted by the violence we've touched upon, there exists an unspoken companion that shadows her every step—the weight of guilt. This isn't just any guilt; it's a heavy burden, an unwelcome guest that takes up residence in the very core of her being.

The guilt mentioned here does not manifest in grand gestures or in a cinematic way, it is manifested in simple daily life tasks, such as in new relationships — not only with others, but with the victim itself. They start to feel afraid of people, of emotional connections, they start to remember episodes and moments where they could have said or done something different, as they had any culpability as victims. The victims start to feel like everyone is planning something against them.

The struggle with guilt isn't just a fleeting emotion—it's a journey through a labyrinth of self-blame, with twists and turns that make it difficult to find the way out. In the aftermath of violence, it becomes an inescapable companion, coloring perceptions, shaping reactions, and casting a long shadow over the path to healing.

Researchers, too, have delved into the intricate link between this pervasive guilt and the psychological aftermath it leaves in its wake. It's not just a standalone emotion; it's entangled with other struggles, like the delicate threads that weave a tapestry of pain. Studies consistently draw connections between this guilt and the complex web of conditions such as dissociation and eating disorders, revealing the nuanced impact on a survivor's mental landscape[50].

Dissociation, a coping mechanism that allows the mind to distance itself from overwhelming emotions, becomes a subtle consequence of this guilt-laden journey. It's a survival tactic, an attempt to create mental barricades against the flood of painful memories. Women navigate the tricky waters of trauma, often unintentionally resorting to mechanisms that help them cope.

And then there's the intricate connection between guilt and the tumultuous world of eating disorders. It's not just about food; it's about regaining control, about reclaiming some semblance of power in the aftermath of a loss. The guilt assumes the role of a tacit

[50] Same as 41.

orchestrator, manipulating the underlying dynamics that contribute to abnormal relations with food, consequently influencing the individual's self-perception[51].

In essence, the aftermath of this type of violence isn't just about scars; it's about the quieter, less visible wounds that linger in the soul. The insidious presence of guilt, woven into the very fabric of psychological consequences, stands as a testament to the enduring impact of such experiences. As we collectively strive for a world free from the chains of violence, let's not forget the subtle battles being fought against this guilt—an acknowledgment that can pave the way for genuine healing and empowerment.

The insidious act of Non-Consensual Pornography, constitutes a deeply troubling form of gender-based violence that extends its harmful reach into the digital realm. This violation of privacy not only inflicts immediate harm but also leaves lasting psychological trauma on its victims, creating a complex tapestry of emotional distress that intersects with broader issues of gender violence.

Non-Consensual Pornography gives rise to an overwhelming sense of betrayal and violation of trust. The intentional sharing of intimate images without consent, often by someone known to the victim, breaches the foundation of trust in personal relationships. This betrayal is not just an isolated incident; it becomes a focal point for understanding the intricate power dynamics and the deeply rooted gender inequalities that contribute to acts of digital abuse.

The emotional fallout from such violations is profound, encompassing pervasive feelings of shame and humiliation. Victims grapple with a sense of inadequacy and self-blame, perpetuated by societal judgments and victim-blaming narratives. This emotional burden, stemming from the violation of personal boundaries, highlights the inextricable link between Non-Consensual Pornography and broader patterns of gender-based violence[52].

For some victims, the trauma associated with Non-Consensual Pornography meets the criteria for post-traumatic stress disorder (PTSD). Intrusive memories, nightmares, and heightened reactivity further underscore the severe and lasting

[51] Idem.
[52] Scarpatto, Salvaro, and Camargo, “Women in Situations of Violation of Privacy.”

psychological impact. These symptoms reflect the intersection between the digital violation of privacy and the enduring consequences of gender violence[53].

In the pursuit of creating a society free from the chains of gender violence, acknowledging and addressing the psychological trauma inflicted by Non-Consensual Pornography becomes a pivotal step. By recognizing the intersections between digital abuse and broader issues of gender-based violence, we lay the foundation for comprehensive efforts that prioritize empathy, consent, and the holistic well-being of individuals affected by these violations.

Moreover, the restriction of social interaction resulting from the dissemination of intimate images is not solely caused by external judgments but is also perpetuated by internalized guilt within the patriarchal structure. The power dynamics within relationships, shaped by patriarchal influences, underscore the control exerted over individuals' lives, especially within the sphere of sexuality.

The narratives in various documents underscore that psychological violence often precedes and follows the improper disclosure of intimate images. This form of violence compromises self-esteem, self-deprecation, and psychological health, creating an intricate web of emotional challenges for survivors. The intensity and duration of suffering caused by such violations are evaluated by the judiciary, recognizing the challenge in quantifying and establishing a monetary value for the moral damage experienced by individuals.

In the quiet corners of an individual's life, far beyond the tangible wounds and emotional bruises inflicted by the violence, there exists an unspoken companion that shadows every step—the weight of guilt. This isn't just any guilt; it's a heavy burden, an unwelcome guest that takes up residence in the very core of one's being.

This guilt doesn't manifest through overt actions; instead, it insidiously infiltrates through the vulnerabilities created by past trauma, settling in the junctures of pain and regret. It subtly reminds individuals of choices that, in hindsight, appear as errors during quiet moments. This guilt persists beyond a momentary emotion; it entails navigating a complex maze of self-reproach, replete with convoluted paths that

[53] Idem.

challenge resolution. Following instances of violence, it becomes an unavoidable companion, influencing perspectives, molding responses, and casting a prolonged shadow on the journey towards recovery.

Some researchers[54] have delved into the intricate connection between this pervasive guilt and the psychological aftermath it leaves in its wake. It's not just a standalone emotion; it's entangled with other struggles, similar to the intricate threads composing a fabric of distress. The same study consistently draws connections between this guilt and the complex web of conditions such as dissociation and eating disorders, revealing the nuanced impact on a survivor's mental landscape.

Dissociation, a coping mechanism that allows the mind to distance itself from overwhelming emotions, becomes a subtle consequence of this guilt-laden journey.[55] It's a survival tactic, an attempt to create mental barricades against the flood of painful memories. In this delicate dance with guilt, individuals navigate the tricky waters of trauma, often unintentionally resorting to mechanisms that help them cope.

2.3 Personality Rights, Privacy Violations and Their Legal Implications

The protection of personality typically involves a group of rights like privacy, identity, and dignity[56]. The term 'personality rights' is expansive, and the protection of these rights is primarily derived from the legal systems of EU Member States. EU law ensures this protection by making reference to the legal sources and systems of each Member State. Definitions of these rights are also provided in the case-law of the European Court of Human Rights (ECtHR), which in its decisions includes aspects related to personality and personal identity in the protection of private life, according to Article 8(1) ECHR, such as a person's reputation, name, or picture.

This is important in cases where a court in a Member State is deciding on personality rights infringements. This is why jurisdiction is significant, as different Member States may have varying rules on how personality rights are configured and

[54] Yoon et al., "Sexual and Physical Abuse and Identity of the Perpetrator."

[55] Caron Zlotnick et al., "The Relationship between Characteristics of Sexual Abuse and Dissociative Experiences," *Comprehensive Psychiatry* 35, no. 6 (1994): 465–70, doi:10.1016/0010-440X(94)90230-5.

[56] Susanna Lindroos-Hovinheimo, "Jurisdiction and Personality Rights – in Which Member State Should Harmful Online Content Be Assessed?," *Maastricht Journal of European and Comparative Law* 29, no. 2 (2022): 201–14, doi:10.1177/1023263X221076392.

how they are protected. Although personality rights do not have the same legal framing across the EU Member States, the Charter of Fundamental Rights of the European Union, and some of the rights described and mentioned in the Charter are:

- The right to the integrity of the person (art. 3.1): “Everyone has the right to respect for his or her physical and mental integrity”.
- Respect for private and family life (art. 7): “Everyone has the right to respect for his or her private and family life, home and communications.”
- Protection of personal data (art. 8): “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.”

The Court of Justice of the European Union (CJEU) has provided perspectives on what they might encompass. Personality rights include the right to privacy, the right to one's own image, the prohibition of defamation, and the protection of a good name and reputation[57]. In jurisdiction disputes, distinctions are sometimes made between violations of privacy and other rights related to personality. Additionally, the EU Court's jurisdiction highlights that personality rights may belong to either a natural person or to a legal person — This diversity in scope and content adds complexity to these rights.

The General Data Protection Regulation aims to empower individuals and give them control over their personal data. While the term "personality rights" is not explicitly mentioned in the General Data Protection Regulation (GDPR), aspects of personality rights, including the right to access their personal data, the right to rectification, the right to erasure (commonly known as the "right to be forgotten"), and the right to object to the processing of their data are disposed on the regulation. They disposed on the following articles:

[57] Lindroos-Hovinheimo, “Jurisdiction and Personality Rights – in Which Member State Should Harmful Online Content Be Assessed?”

- Article 15 of the GDPR[58]: "The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: The purposes of the processing; The categories of personal data concerned; The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject, or to object to such processing; Where the personal data are not collected from the data subject, any available information as to their source."

- The right to rectification is disposed on the article 16: "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

- Right of erasure (right to be forgotten) on the article 17: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to

[58] https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e2244-1-1

which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

- Right to restriction of processing on the article 18: "The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State."

On the third chapter, the regulation talks about the rights of the individual and the Recital number 59[59] is disposing about the procedures for the exercise of the Rights of the Data Subjects: "Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object." This means that the processing of personal data and informations should be clearly explained, including the purposes of processing, the categories of data being used and also possibly of erasure of a data.

In essence, while the term "personality rights" may not be explicitly used, the GDPR provides a comprehensive framework for protecting the privacy and rights of individuals in the context of personal data processing, thus providing a sense of security and autonomy regarding the usage and processing of personal information.

[59] Available here: https://eur-lex.europa.eu/eli/reg/2016/679/oj

When it comes to Brazilian law, we could see a gap in the jurisdiction and regulations, as the Civil code of 1916 did not even mention personality rights in any way. The Federal Constitution published in 1988 regulated in its article 5, X that:

"All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: X - the privacy, private life, honor and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured." [60]

To align with that, the Civil Code published in 2002 regulated the personality rights as a series of prerogatives inherent to the human person, aimed at protecting essential aspects of individuality. Those rights include aspects such as life, physical and moral integrity, honor, image, privacy, name, and other elements that constitute an individual's identity. With technological advancements and the importance of personal data protection, issues related to privacy and information protection have gained prominence in the Brazilian legal system. The Law of Access to Information (12.527/2011), Habeas Data Law (Decree 7.962/2013), Consumer Law (8.078/1990), the Marco Civil da Internet, came before so the Lei Geral de Proteção de Dados (Law No. 13.709/2018, hereinafter LGPD) could complement and regulate in the context of digitalization and personal data.

The LGPD establishes a series of rules and principles to guarantee the protection of data. These principles align with the broader protection of privacy and personal rights outlined in the Civil Code. In terms of consent and control, the LGPD introduces specific provisions to regulate the obtaining of consent for data processing, empowering individuals with more control over their personal information — such as the right to access, rectify, add or port their data. Also, and maybe more important, the LGPD regulates the obligations of companies and how they keep and store personal data, this way, they could be accountable for data processing activities.

[60]Brasil Constituição (1988) Emendas, "Constitution of the Federative Republic of Brazil : Constitutional Text of October 5, 1988, with the Alterations Introduced by Constitutional Amendments No. 1/92 through 72/2013 and by Revision Constitutional Amendments No. 1/94 through 6/94," 2013, https://www2.senado.gov.br/bdsf/handle/id/243334.

With regard to data breach notification, the LGPD introduces requirements for timely notification in the event of a security incident. This provision contributes to the protection of individuals' rights of personality by providing transparency and aligning with international regulations about data and information.

In summary, the Federal Constitution, the LGPD and the Civil Code together create a legal framework for the protection of personal rights in Brazil. While the Federal Constitution embraced, protected, and sanctioned the personality rights considering the dignity of the human person as a fundamental principle of the Federative Republic of Brazil, the Civil Code and the LGPD provide a specialized and detailed legal framework to complement the provision creating a complete legal framework on the Brazilian legislation.

2.4 Fighting Non-Consensual Pornography: Recent examples around the world

It’s not difficult to find examples of privacy violations in the context of Non-Consensual Pornography, they can be from a neighbor, a family member, a friend or even a colleague, all of them carry the damages and traumas caused by this type of violence.

In 2011, Carolina Dieckmann, a famous actress in Brazil, had her computer hacked by a group who got access to her personal informations and pictures, they said that she had to pay R$10,000 (ten thousand Brazilian reais) — the equivalent to 1,878.96 euros[61] — to avoid the publication of the pictures. She did not pay, and they exposed more than 30 personal pictures of her on the internet. The repercussions of the case were huge, and they saw the need to create a special law and to make the extent regulations harsher to make sure that the victims were protected in the best way possible.

In order to ensure security in the virtual environment, in the same year, six federal deputies proposed a bill to address electronic device invasions and the use of obtained information. The proposed legislation aimed to address crimes resulting from

[61] Exchange rate of the 27th of December 2023.

the improper use of information and personal materials related to the privacy of any individual on the internet, such as photos and videos. The bill was reviewed by senators, who emphasized the need for the measure to also combat electronic financial fraud.

Senator Eduardo Braga, from the Amazonas state and a member of the MDB, served as the rapporteur for the proposal in the Science and Technology Committee. He noted that until the project's vote in 2012, there was no specific provision in the criminal legislation for computer crimes, including the capture of credit or debit card data that facilitates counterfeiting. He highlighted the damages that had been growing in Brazil since then. The law sanctioned in 2012 established a period of 120 days before coming into effect.

Therefore, since March 2012, the country has had a law criminalizing the invasion of mobile phones, computers, or computer systems to obtain, alter, or destroy data with the aim of gaining an illicit advantage. This may also be the objective of invading computer devices to install vulnerabilities. The penalties specified in the Carolina Dieckmann Law for this crime saw a significant increase in 2021 when another legislation on the subject came into effect based on a proposal by Senator Izalci Lucas from the PSDB party in the Federal District[62].

The punishment, which originally ranged from three months to one year of imprisonment and a fine, was amended to imprisonment for one to four years and a fine. The same penalty applies to those who produce, offer, distribute, sell, or disseminate a device or computer program for committing the crime. Izalci Lucas's proposal was introduced during the COVID-19 pandemic, a period in which, as the senator emphasized, the number of electronically committed frauds increased drastically, resulting in losses for consumers and businesses.

Izalci also suggested imprisonment for four to eight years and a fine for electronic fraud committed using information provided by the victim or by a third party induced into error through social media, phone contacts, or fraudulent email. The project's rapporteur, Senator Rodrigo Cunha from União de Alagoas, confirmed the

[62] "Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos," *Rádio Senado*, accessed January 21, 2024, https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos.

increase in crimes in the country during the health emergency. Another addition to the penalties determined by the Carolina Dieckmann Law pertains to individuals who invade computer devices and gain access to private electronic communications, commercial or industrial secrets, confidential information as defined by law, or remote control of the invaded device. The punishment, which was initially imprisonment ranging from six months to two years and a fine established in 2012, was increased to imprisonment for two to five years and a fine starting in 2021.[63]

A recent article published by The New York Times explored the fact that Canada still allows MindGeek (the company that owns the website PornHub) to profit with Non-Consensual Pornography and other contents in their website. One of the cases reported on the website was the one of Serena K. Fleites. She was a student of 14 years old when she sent a video to a guy and he spreaded the content with other colleagues and someone uploaded the content on PornHub. She started to receive threats and had to change schools because of the shame and the guilt she was feeling. After they got in touch with the website, the content/video was deleted/removed, but after a few days it was uploaded again by someone else and to other websites as well. She attempted suicide twice, developed an addiction to meth and opioids, and at 16 she started to sell naked pictures and videos of herself as she dropped out of school and became homeless. She declared[64]: "I'm not worth anything anymore because everybody has already seen my body.". Not only that, but she was afraid of applying for fast-food jobs because one of the videos of when she was only 14 had already 400,000 views and someone could recognize her.

PornHub is a problematic website, as bad as the others available, that profit from the suffering and exploitation of the image of women including young girls. A petition launched in February 2020 organized by a worldwide movement with the single purpose of shutting down Pornhub and holding its executives accountable for enabling, distributing and profiting from Non-Consensual Pornography and other crimes broadcasted on that platform. The petition[65] already counts with 2,323,216 (two million three hundred twenty-three thousand two hundred sixteen) signatures at this date.

[63] "Dez anos de vigência da Lei Carolina Dieckmann."

[64] Nicholas Kristof has been a columnist for The Times since 2001. He has won two Pulitzer Prizes, for his coverage of China and of the genocide in Darfur. The article can be found here: https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html

[65] The petition can be found here: https://traffickinghubpetition.com

A study conducted[66] across the UK, Australia and New Zealand in between 2017 and 2020 presented data from 75 victims of Non-Consensual Pornography. Participants in the study reported a wide range of experiences related to image-based sexual abuse. A significant majority disclosed instances where their nude or sexual images were distributed without consent, involving scenarios such as consensual sharing, non-consensual photography, and being unaware of being filmed or photographed. Many described how these images were disseminated through mobile phones, apps, pornographic websites, social media, chat rooms, or image board sites. Threats to share such images were common, often aimed at exerting control through coercion, such as blackmail, demanding money, or pressuring victims into unwanted actions. Some participants had images taken without agreement, sometimes while asleep, under the influence of substances, or with hidden cameras. A few reported digital alterations to make them appear nude or sexual.

Perpetrators were overwhelmingly identified as men, and some victims experienced multiple instances of abuse by the same or different perpetrators, often in conjunction with other forms of sexual violence, domestic abuse, stalking, and harassment, both online and offline. Nearly one-third of participants experienced image-based sexual abuse alongside or within the context of domestic abuse. The abuse disrupted their lives profoundly, altering their sense of self and relationships. They viewed victimization as a point of fracture, causing far-reaching changes and a distinction between 'before' and 'after' the abuse. Despite individual differences, the impact was universally perceived as an extreme violation, affecting personal, professional, and digital aspects of their lives. [67]

And last, it’s important to talk again about the websites created only for Non-Consensual Pornography purposes, such as MyEx.com and IsAnyoneUp.com. The creator of the second website mentioned gained some more attention after the documentary “The Most Hated Man on the Internet” was released on Netflix. Hunter Moore was self-dubbed King of Revenge Porn and created this platform that featured Non-Consensual Pornography content that could be uploaded anonymously and with

[66] Clare McGlynn et al., “‘It’s Torture for the Soul’: The Harms of Image-Based Sexual Abuse,” *Social & Legal Studies* 30, no. 4 (2021): 541–62, doi:10.1177/0964663920947791.

[67] Erika Rackley et al., “Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse,” *Feminist Legal Studies* 29, no. 3 (2021): 293–322, doi:10.1007/s10691-021-09460-8.

personal information of the victims — he claimed that the website was attracting more than 30 million monthly page views.

The website was shut down in 2012 after the website was sold to McGibney, an anti-bullying advocate and Moore was convicted in a federal court on charges of conspiracy and unauthorized access to protected computers several times and was sentenced to two and a half years in federal prison, followed by 3 years of supervised release. While IsAnyoneUp.com may have been shut down, the concept of digital revenge porn unfortunately still exists across social media platforms or in corners of the dark web.

The thing present in every case and situation where privacy is violated in the context discussed previously in this research is that the trust is broken, and the control is, most of the time, on the hands of the aggressor. This aggressor can be anyone. Can be the owner of a Non-Consensual Pornography website that is seen as a visionary by influential magazines and communication companies. The ex-boyfriend that does not understand the reason why he could not expose someone that once was their partner. Someone that does not even know the victim, but they know that they have the power to destroy reputations, trust, and mostly have control of an unfair narrative that causes pain, traumas and violates fundamental rights of the victims.

2.5. Privacy and Data Protection in the EU

The historical evolution of the privacy concept can be understood by analyzing different events and facts. Since 1948 with the creation of the Universal Declaration of Human Rights and the definition of the protection of privacy of individuals and families found the article 12th: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[68] It is seen as the starting point and the inspiration for all the subsequent legislations created to protect personal data not only on the real world, but now, also on the digital world. And as mentioned, after, countries such as Denmark (Act no. 429 of 31/05/2000), France (Law No. 78-17 of January 6, 1978), Germany (*Bundesdatenschutzgesetz,* officially published on July 5, 2017), Norway (*Forskrift til*

[68] Available here: https://www.ohchr.org/en/human-rights/universal-declaration/translations/english

personopplysningsloven published on the 1st of January of 2001) and others approved national laws of privacy creating a certain sense of disparity as this was not something that followed a standard.

So two decades ago, practically in the pre-internet era when data was valuable but a bit harder to gather, the European Commission saw the need for alignment between the member states regarding data privacy in order to facilitate, in a certain way, transactions of data between the states. The problem was that even having internal regulations, they also had different levels of regulated actions and protections, causing a certain instability and uncertainty between the individuals and the data controllers and processors, as noted by Polenz and highlighted by Voigt et al[69]. After this, in 1995, Europe adopted the 95/46/EC Directive regarding the processing of personal data and other factors involved.

In 2016, the European Union adopted the General Data Protection Regulation. The need of certainty between the data handling in the countries were bringing insecurities not only to individuals but also to the economic activities at EU level. So the creation of this regulation is not important only for economic reasons, but also to ensure and regain people's trust on the treatment of their data[70].

The GDPR maintains a lot of the elements disposed in the Directive, but it also adds different elements, specially three: more severe sanctioning regime, the right to be forgotten and the mandatory assignment of a Data Protection Officer.[71] It is applied as a general law to be applied in a diverse background of actors and situations — involving public bodies and private organizations[72].

The General Data Protection Regulation has explicitly prescribes the principles that should be respected when personal data are processed. They are[73]:

---

[69] Polenz S (2013) Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes. In: Kilian W, Heussen B (eds) Computerrechts-Handbuch, supplement 8/2013. C.H. Beck, Munich on Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing, 2017), doi:10.1007/978-3-319-57959-7.

[70] Paul Voigt and Axel Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing, 2017), doi:10.1007/978-3-319-57959-7.

[71] Christopher F. Mondschein and Cosimo Monda, "The EU's General Data Protection Regulation (GDPR) in a Research Context," in *Fundamentals of Clinical Data Science*, ed. Pieter Kubben, Michel Dumontier, and Andre Dekker (Cham: Springer International Publishing, 2019), 55–71, doi:10.1007/978-3-319-99713-1_5.

[72] Idem.

[73] Article 5 available here: http://data.europa.eu/eli/reg/2016/679/oj

Lawfulness, fairness and transparency (art. 5.1.a): "Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject"

- Lawfulness in personal data processing requires compliance with GDPR, having a legal basis, and avoiding unlawful processing. Fairness mandates treating individuals' data fairly, avoiding harm or deception. Transparency it means that the regulation demands clear communication to individuals and regulators about data processing. Controllers must provide concise, easily accessible, and understandable information before and after data collection, following specific rules in Articles 12, 13, and 14 GDPR — Transparency involves informing individuals about processing existence and purposes, using appropriate means for the platform and audience. [74]

Purpose limitation (art. 5.1.b): "Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."

- When collecting personal data for specific purposes, avoiding incompatible processing, controllers can engage in additional processing for archiving, public interest, scientific, historical, or statistical purposes with safeguards. The regulation outlines rules for public interest processing. Compatibility for further processing depends on the link to the original purpose, context, nature of data, consequences, and safeguards. This principle ensures transparency, aligning with individuals' expectations and supporting data minimization and accountability.[75]

Data minimization (art. 5.1.c): "Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"

- Requires organizations to only collect and process the personal data that is truly necessary for their intended purposes. It means gathering the least amount of

[74] "Principles of Data Protection | Data Protection Commission," *Principles of Data Protection | Data Protection Commission*, accessed January 13, 2024, https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection.

[75] Idem.

data required and avoiding unnecessary information. By doing so, organizations enhance data protection, reduce the risk of data breaches, and ensure the accuracy and currency of the information they hold. Regular reviews are recommended to ensure ongoing compliance and to remove outdated or unnecessary data.[76]

Accuracy (art. 5.1.d): "Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

- Data controllers maintain the accuracy of personal data and promptly rectify any inaccuracies, ensuring alignment with the intended purposes of data processing. It straightforwardly requires all collected or stored personal data to be accurate and current. Controllers must proactively take reasonable measures to correct inaccuracies, potentially necessitating periodic updates. Clear procedures for data correction or erasure should be established as part of the overall data management process. The specific steps required for accuracy maintenance depend on the nature of the data and processing activities. Controllers should also be mindful of data subjects' right to rectification, allowing individuals to correct or complete inaccurate personal data.[77]

Storage limitation (art. 5.1.e): "Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject"

[76] "Principles of Data Protection | Data Protection Commission," *Principles of Data Protection | Data Protection Commission*, accessed January 13, 2024, https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection.

[77] Idem.

- Controllers must retain personal data, allowing individual identification, only for the duration necessary for the intended processing purposes. Exceptions include storing data for public interest archiving, scientific research, historical research, or statistical purposes, provided appropriate measures safeguard individuals' rights. Generally, personal data should be deleted once it's no longer needed, with controllers establishing time limits or periodic reviews. Transparency is key; controllers must inform individuals of retention periods or criteria. Even offline or manual data storage requires justification and compliance with data subject requests. Depending on circumstances, anonymizing data when identification is unnecessary may be appropriate, but true anonymity occurs only when the individual is no longer identifiable. Pseudonymized data, still considered personal, may be reversible, and the process for anonymizing must be permanent.[78]

Integrity and confidentiality (art. 5.1.f): "Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures"

- Personal data must be processed securely and confidentially by controllers. This involves protecting it from unauthorized processing, accidental loss, destruction, or damage. Controllers must use appropriate technical or organizational measures, covering cybersecurity, physical, and organizational security. Regular updates and checks are necessary to ensure the effectiveness of these security measures. While the GDPR doesn't specify particular measures, controllers should consider various options based on evolving best practices. Factors like data minimization, data protection principles, transparency, and encryption should be considered when choosing security measures.[79]

Accountability (art. 5.2): "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1"

---

[78] "Principles of Data Protection | Data Protection Commission," *Principles of Data Protection | Data Protection Commission*, accessed January 13, 2024, https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection

[79] Idem.

- The accountability principle in data protection law states that controllers must follow and prove compliance with other data protection principles. This involves having processes and records in place. Adhering to principles like data protection by design, using proper measures, providing clear information, and having data retention policies supports accountability. Controllers can appoint a data protection officer, maintain processing records, establish clear contracts, and conduct impact assessments. Compliance is an ongoing obligation, requiring regular review and updates of accountability measures.[80]

The regulation provides precise legal definitions for certain terms, one of them, crucial for the discussion in this study is the one of Personal Data, in the first chapter, article 4.1[81] it says: "'*personal data' means any information relating to an identified or identifiable natural person ('data subject')*; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Another important definition is present at the article 4.2: "'*processing'* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as *collection, recording*, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"

These two definitions, of personal data and what is considered to be processing by the GDPR, are crucial to understand the Non-Consensual Pornography discussion in this study. When the GDPR defines personal data and what can be considered processing, we can understand the application of the relevant regulation to protect victims and expect accountability from those who share, record, collect and storage data without consent.

---

[80] "Principles of Data Protection | Data Protection Commission," *Principles of Data Protection | Data Protection Commission*, accessed January 13, 2024, https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection

[81] Available here: https://eur-lex.europa.eu/eli/reg/2016/679/oj

On article 17 of the same regulation, we can see how the right to erasure (right to be forgotten) can be applied in certain situations, in particular when: “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f)the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).”

The first time that the right to be forgotten was mentioned in the European Union was in May 2014 in the Google Spain SL v Agencia Espanola de Protecctión de Datos & Mario Costeja González when the justice decided that Google should hide all the irrelevant data of the subject, the decision was made based on the fundamental right to privacy of an individual. Following the judicial recognition of the right to be forgotten, Google filed a lawsuit against CNIL (Commission Nationale Informatique & Libertés, is the French Data Protection Agency), arguing that the right should not be globally enforced but limited to the territory of the European Union. Google's contention was supported by the Advocate General of the European Court of Justice, who ruled that the right to be forgotten should indeed be confined to the European Union. The Court sided with Google, emphasizing that the right is not absolute, and the data controller is responsible for delisting content from the European versions of websites. However, the content remains accessible to individuals outside the European Union.

It's worth emphasizing that this legislation not only defines the parameters and provisions governing data protection but also elucidates the pathways through which individuals can assert their rights in safeguarding their personal information. The

meticulous articulation of these dispositions within the law not only provides clarity but also establishes a standard framework for addressing data protection concerns. Importantly, the GDPR's inspired other nations to develop and implement similar frameworks to regulate and protect data in a consistent and effective manner.

2.6. Privacy and Data Protection in Brazil

In 2014 the first specific regulation that could protect users in the digital world was promulgated in Brazil. It was called Marco Civil da Internet (MCI) — Law 12.965/2014. It was considered the Constitution of the Brazilian Internet, as it brings the definitions and principles that regulate the digital activities in the country. One important thing to mention is that, since the Marco Civil was a new legislation regarding this kind of laws and rights, it did not have a list of definitions or specific scenarios, it was more like a general approach with principles to regulate the digital activity in Brazil[82].

The concept of privacy was already defined by other regulations, in particular the Federal Constitution (art. 5, X), the Law of Access to Information (12.527/2011), Habeas Data Law (Decree 7.962/2013), Consumer Law (8.078/1990), the MCI as mentioned before and others. However, privacy and data protection are different and that's why the Lei Geral de Proteção de Dados was created in 2018, highly inspired by the GDPR; its main purpose was to protect personal data of natural persons.

The structure of the act is very similar as well, the first chapter of the LGPD makes general dispositions about the law, states clearly the principles applied and the definitions of some important terms that will be used in the text. The first definition that it's important to mention is the one of Personal Data that can be found on article 5 of the LGPD: "personal data: information related to *natural person identified or identifiable*", another important definition is the one of sensitive personal data on the second paragraph of the same article: "personal data, on racial or ethnic origin, religious convictions political opinion, affiliation to a union or organization of a religious

[82] Pedro Andrade Guimarães Filho, Ariê Scherreier Ferneda, and Miriam Olivia Knopik Ferraz, "A Proteção De Dados E A Defesa Do Consumidor: Diálogos Entre o CDC, O Marco Civil Da Internet e a LGPD," *Revista Meritum* 15 ed 2 (2020), doi:10.46560/meritum.v15i2.7749.

philosophical or political nature, *data relating to health or sexual life*, genetic or biometric data, when linked to a natural person."

The other important definition on the law is regarding the processing of Data in the digital world, it can be found on the same article, on the paragraph 10: "Data processing is considered any activity that uses personal data in the execution of its operations, such as: *collection, production*, reception, classification, *use, access, reproduction, transmission, distribution*, processing, filing, storage, elimination, evaluation, or control of information, modification, communication, *transfer, dissemination, or extraction.*"

The principles are explained and classified on article 6 of the Lei Geral de Proteção de Dados, good faith in the handling of personal data is a fundamental premise. Additionally, it is necessary to ponder questions such as "What is the purpose of this data processing?", "Is it really necessary to use this amount of data?", "Has the individual I am interacting with given consent?", and "Could the use of the data lead to any form of discrimination?". They are:

Purpose limitation[83] (art. 6. I): "Processing done for legitimate, specific and explicit purposes of which the data subject is informed, with no possibility of subsequent processing that is incompatible with these purposes"

- The processing and treatment of the data should be for a valid, clear, and well-defined reason previously communicated to the individual. There should be no chance of using the information in a way that goes against these initially stated purposes.

Adequacy (art. 6. II): "Compatibility of the processing with the purposes communicated to the data subject, in accordance with the context of the processing"

- The processing of data should align with the purposes communicated to the individual, considering the context of the processing.

[83] Translation of the articles and the LGPD provided by Rennó Penteado Sampaio Advogados here: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

Necessity (art. 6. III): “Limitation of the processing to the minimum necessary to achieve its purposes, covering data that are relevant, proportional and non-excessive in relation to the purposes of the data processing”

- The handling of data to the minimum necessary for achieving its intended purposes. The data collected should be relevant, proportional, and not excessive in relation to the goals of the data processing.

Free access (art.6. IV): “Guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data”

- Individuals should have easy and free access to information about how their personal data is being processed, including details about the method, duration, and entirety of their data.

Quality of the data (art. 6. V): “Guarantee to the data subjects of the accuracy, clarity, relevancy and updating of the data, in accordance with the need and for achieving the purpose of the processing”

- Individuals whose data is being processed are provided with a guarantee that the information is accurate, clear, relevant, and up-to-date. It emphasizes the importance of maintaining the precision and currency of data in line with the intended purpose of the processing. The goal is to meet the specific needs of data processing and to ensure that individuals have reliable and current information about them.

Transparency (art. 6. VI): “Guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy”

- Ensure that individuals have access to transparent, accurate, and easily available information about how their data is being processed and who is handling the processing, while still respecting commercial and industrial secrets.

Security (art. 6. VII): "Use of technical and administrative measures which are able to protect personal data from unauthorized accesses and accidental or unlawful situations of destruction, loss, alteration, communication or dissemination."

- Employing technical and administrative measures to safeguard personal data against unauthorized access, as well as accidental or unlawful incidents such as destruction, loss, alteration, communication, or dissemination.

Prevention (Art. 6. VIII): "Adoption of measures to prevent the occurrence of damages due to the processing of personal data."

- Implementing preventive measures to avoid any negative consequences or harm resulting from the processing of personal data. This includes actions like securing data against unauthorized access and regularly checking for vulnerabilities, promoting responsible data handling practices, and ensuring compliance with privacy regulations.

Nondiscrimination (Art. 6. IX): "Impossibility of carrying out the processing for unlawful or abusive discriminatory purposes"

- Ensuring that the handling of personal data is strictly prohibited for any purposes that are deemed illegal, abusive, or discriminatory. This includes implementing measures to actively prevent and prohibit the utilization of such data for activities that violate the law, go against ethical standards, or involve any form of unfair treatment. This commitment underscores the importance of maintaining the integrity and ethical use of personal information, promoting a responsible and lawful approach to data processing.

Accountability and transparency (Art. 6. X): “Demonstration, by the data processing agent, of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures.”

- The entity is required to exhibit, through evidence, the implementation of effective measures that demonstrate adherence to and compliance with regulations related to the protection of personal data. Additionally, they should be able to prove the effectiveness of these measures in ensuring the proper safeguarding and responsible handling of personal information. This emphasizes the importance of not only having policies in place, but also being able to substantiate their practical effectiveness in practice.

Also, the LGPD mentions in its article 18 a variation of the “right to be forgotten”: The data subject has the right to obtain from the controller, in relation to the data processed about the data subject, at any time and upon request:[…] IV - anonymization, blocking, or *elimination of unnecessary, excessive, or data processed in violation of this Law.*" where it can be seen a broader definition of this right, which can cause conflicts with the existent regulation in the country. By approaching the issue from a voluntarism perspective, where facts related to an individual are subjected to their personal will, the right to be forgotten takes on proprietary characteristics, incompatible with the Brazilian constitutional order, which protects freedom of information and access to information for society as a whole, not only as fundamental rights but also as prerequisites of a Democratic State[84].

On the other hand, the regulation is explicit saying that consent is the main basis of this law, disposing that is valid when: “is a free, informed, and unequivocal expression through which the data subject agrees to the processing of their personal data for a specific purpose.”

It’s clear that some concepts and rights caused discussion and doubts in the Brazilian judiciary system because of its broad terms and definitions. The Brazilian

[84] Gustavo Tepedino, Ana Frazão, and Milena Donato Oliva, “Lei geral de proteção de dados pessoais: e suas repercussões no direito brasileiro,” 2023, https://bdjur.stj.jus.br/jspui/handle/2011/139297.

legislation, following the European model, introduces state regulation over a reality that has emerged with contemporaneity. The self-regulated ethics of digital network operators and digital marketing companies now face a new level and must adapt to this reality.

In the current context of digital evolution, we live in a world where targeted advertising emerges daily on the screens of citizens' smartphones and computers. Consequently, personal information becomes increasingly valuable as a product and a bargaining chip. Measures such as the creation of the LGPD are necessary for the healthy social development, both within the virtual world and beyond[85].

2.7. Approaches to Valid Consent and Regulatory Gaps in the GDPR and in the LGPD

Consent is a term that has been causing discussions and concerns for decades, as it has different meanings. Basically, consent can be given by someone that is able to make a moral decision about what is being consented to, if someone is not able to understand or does not know what they are agreeing to, then the consent is not valid. Competence is a prerequisite for giving consent, which should be willingly and freely provided, devoid of coercion. This necessitates a foundation of understanding, assuming that the individual granting consent is well-informed, and the act of consenting is a deliberate and intentional choice[86]. This term is so important that it was the main reason why the name “revenge porn” was changed in the first place — The lack of consent and the exposure are the main things that make Non-Consensual Pornography, a nightmare for the victims as the control of the narrative is not on their side.

The GDPR in its recital 43 states that consent should be clearly indicated for a specific purpose: *“2. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including*

[85] Maria Eugenia Finkelstein and Claudio Finkelstein, “Privacidade e Lei Geral De Proteção De Dados Pessoais,” *Revista de Direito Brasileira* 23, no. 9 (February 11, 2020): 284, doi:10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343.

[86] Franklin Miller and Alan Wertheimer, eds., *The Ethics of Consent: Theory and Practice*, 1st ed. (Oxford University PressNew York, 2009), doi:10.1093/acprof:oso/9780195335149.001.0001.

the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

Consent in data processing, according to the GDPR, demands freely given, specific, and *informed* agreement, avoiding coercion. It should entail an unambiguous indication of wishes, be auditable for future-proof, allow easy withdrawal, and explicitly outline the consented terms for verification. This entails individuals providing an unambiguous indication of their wishes, ensuring that their agreement can be audited for future reference and accountability. Moreover, individuals must have the ability to withdraw their consent easily and at any time.[87]

When it comes to the Brazilian regulation, article 5 paragraph XII of the LGPD, states that consent should be "free, informed and unambiguous manifestation whereby the data subject agrees to the processing of personal data for a given purpose". After the definition of the term, the LGPD considers consent as one of the scenarios legitimizing the processing of personal data. In fact, the scenario outlined in Article 7, paragraph I, of the LGPD is the only one where the data subject agrees to the processing of personal data; the other scenarios in the article do not require user consent and, in some cases, pertain to compulsory processing of it[88].

The Lei Geral de Proteção de Dados grants special protection to certain information about individuals. Due to this perspective, it has adopted a broad concept of personal data: "information related to an identified or identifiable natural person." Data that may seem irrelevant at a given moment or does not directly reference someone can, when transferred, combined, or organized, lead to highly specific information about a particular individual, including sensitive details. Recognizing the importance of this matter, a general rule (Article 1) has been established, stating that anyone processing data, whether a natural or legal person, public or private entity, including in digital activities, must have a legal basis to justify their actions.[89]

---

[87] Stephen Breen, Karim Ouazzane, and Preeti Patel, "GDPR: Is Your Consent Valid?," *Business Information Review* 37, no. 1 (2020): 19–24, doi:10.1177/0266382120903254 and Ana C. Carvalho, Rolando Martins, and Luis Antunes, "How-to Express Explicit and Auditable Consent," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)* (2018 16th Annual Conference on Privacy, Security and Trust (PST), Belfast: IEEE, 2018), 1–5, doi:10.1109/PST.2018.8514204.

[88] Dhiulia de Oliveira Santos, "A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018)," September 25, 2019, http://repositorio.uniceub.br/jspui/handle/prefix/13802.

[89] Gustavo Tepedino and Chiara Spadaccini De Teffé, "O Consentimento Na Circulação de Dados Pessoais," *Revista Brasileira de Direito Civil* 25, no. 03 (2020), doi:10.33242/rbdc.2020.03.005.

The Brazilian Civil Code outlines the defects in consent, including error or ignorance (article 138), fraud (article 145), coercion (article 151), state of danger (article 156), and harm (article 157). In the context of consent issues related to personal data processing, a broader concept is adopted, encompassing provisions from LGPD Article 8, paragraph 4: “Consent shall refer to particular purposes, and generic authorizations for processing personal data shall be considered void.” and article 9, paragraph 1: “In situations where consent is required, it shall be considered void if the information provided to the data subject contains misleading or abusive content or was not previously presented in a transparent, clear and unambiguous way”.

These nullify consent in cases of generic authorizations for data processing and when provided information is deceptive, abusive, or lacks prior transparent presentation. Consent for processing can be revoked at any time, as stipulated in LGPD Article 8, paragraph 5: “Consent may be revoked at any time, by *express request of the data subject, through a facilitated and free of charge procedure,* with processing carried out under previously given consent remaining valid as long as there is no request for deletion”.

There are some differences between the regulations analyzed by this research[90]. According to the GDPR requests must be addressed promptly, within one month, and may be extended by an additional two months under certain circumstances; the data subject must be informed of any extensions within one month of the request; data controllers need mechanisms to verify the identity of the requester. Methods of submitting requests include writing, oral communication, and electronic means. Exceptions to the right of deletion include public health, legal claims, and private, non-economic processing. On the other side, according to the LGPD, controllers must respond immediately or provide reasons for delayed action, and there is no requirement for mechanisms to identify the data subject. The right to deletion is exercised through an express request, with additional exceptions for specific data processing purposes.

The main gap found in the context of both data protection regulations analyzed in this research is the emphasis on consent as a fundamental aspect of data processing, aligns with international best practices in privacy and data protection. Consent serves as

[90] European Commission. "Data Guidance: GDPR and LGPD." Futurium, https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf. Accessed January 13, 2024.

a crucial mechanism for individuals to exercise control over their personal information, ensuring that their data is handled in a manner aligned with their preferences.

It is notable that the law doesn't fully adopt a reversal of the burden of proof, a concept where the burden of proving compliance shifts from the individual to the data processor or controller. Instead, it introduces the concept of joint responsibility, implying that multiple parties involved in data processing share accountability.[91]

Even with notable gaps and differences between both regulations, it is crucial to understand their importance and significance for the victims of Non-Consensual Pornography. With those regulations they can see a way to find justice and to get back the control of the narrative and of their data, leveraging the right of erasure (right to be forgotten) and even copyright laws to track and delete data from the digital world, those possibilities will be discussed in the next chapter.

[91] Ribeiro De Menezes Souza, Luíza. 2018. "Proteção De Dados Pessoais: Estudo Comparado Do Regulamento 2016/679 Do Parlamento Europeu E Conselho E O Projeto De Lei Brasileiro N. 5.276/2016". *Caderno Virtual* 1 (41). https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153.

Chapter 3
Case Studies and Comparative Analysis

3.1. Role and Limits of Legislations in Combating Non-Consensual Pornography

More than thirty years ago what we know as “internet” was developed with the main purpose, of being an easy tool to exchange informations between scientist and academic all over the world, in 1993 it was made available for the public in general. Presently, when connected to this high-speed, globally interconnected information network, individuals can effortlessly complete routine tasks and more. Rapid and effective online search engines grant immediate access to a vast array of information. Social networking and communication platforms facilitate the exchange of knowledge with people from various parts of the globe. For entertainment purposes, individuals can readily "stream" a diverse range of online media, including music, videos, and games, on demand. The introduction of portable and versatile "smart" devices further enables constant connectivity, allowing users to seamlessly enjoy multiple Internet-related conveniences simultaneously or switch between them effortlessly. This unparalleled Internet environment, with its diverse capabilities, has significantly reshaped our thoughts and behaviors.[92]

This technology also changed the way that violence can be manifested, spread and shared. The term used by scholars is: Technology-facilitated violence and abuse (TFVA), that is used to describe the use of digital technologies to perpetrate interpersonal harassment, abuse and violence[93]. One example of this is the crime discussed along this research that have been desolating thousands of women around the world.

But on the other hand, with the improvements made online and how valuable data became over the years, regulations also changed and were updated. In 2014 the

[92] Kep Kee Loh and Ryota Kanai, “How Has the Internet Reshaped Human Cognition?,” *The Neuroscientist* 22, no. 5 (2016): 506–20, doi:10.1177/1073858415595005.

[93] Nicola Henry and Anastasia Powell, “Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research,” *Trauma, Violence, & Abuse* 19, no. 2 (2018): 195–208, doi:10.1177/1524838016650189.

Court of Justice of the European Union took the first step in the creation and application of the Right to be Forgotten, even before the existence of this right being properly disposed by the GDPR that was published and approved two years later. [94] This could have been seen as a first promising step to address and to fight back against this modern way of violence.

However, there are some limits regarding the application of the right to erasure, as the freedom of expression and information should also be respected as the fundamental rights that they are. As the text of the Charter of Fundamental Rights of the European Union explains:

- Freedom of Expression and information (article 10): "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

This remains a problem as the victims cannot always count with the regulations to safeguard their privacy and security of their data.

One of the main challenges faced by the victims and the courts when addressing this issue is that the online world can make possible the upload of images by anonymous users, making it extra difficult to find the perpetrators and hold them accountable for their crimes on the digital world. This was discussed in a very serious way when the article "The Children of Pornhub" was published by The New York Times. The main issue here was that anyone, without any kind of identity verification, could upload content to the website. Not only that, but the videos could also be downloaded by the viewers perpetrating the violence and the pain, as they never knew when, how or if that content would disappear.

After the publication of the article, the companies Visa and Mastercard announced that they would stop processing payments to those platforms as they hosted illegal content. In 2019 the company hired a workforce to audit the content uploaded to the platform occasionally, filters were used to avoid the publication of rape tapes, child sexual abuse and the torture of animals. Another problem that caused huge gaps when

[94] Tna Nguyen, "European 'right To Be Forgotten' As A Remedy For Image-Based Sexual Abuse: A Critical Review," *KnowEx Social Sciences*, July 25, 2022, 59–72, doi:10.17501/27059901.2021.2105.

addressing this kind of crimes is that those companies didn't involve the police or law enforcement when they received the content because the people who made the upload were using tools to hide information that could lead to them, causing the eventual targeting of the wrong person.

After the publication of the article, the Canadian Government, the place where it is located the MindGeek headquarters, established a committee requesting information and relevant measures to avoid the perpetration of violence within the platform. It was not only revenge porn the issue, but the upload of rape videos, violence and exposition of minors without accountability from those who committed the crimes, as they couldn't be found because no verification was requested during the uploading process.

PornHub used to receive more website traffic than Amazon and Netflix in 2020[95], and based on the Audio Visual Media Sharing Services Directive (AVMSD) on the Article 1 conceptualizes: "Services whose principal purpose is to provide programmes, user-generated videos, or both, to the general public" they would fit on the description of a platform that is under the AVMSD. The European Union framework for regulating content (DSA) should be applied to them. However, the structure of those companies are usually complicated and layered. MindGeek for example, exhibits intricacy, characterized by a multitude of subsidiaries distributed globally, the nomenclature of which may obscure their ownership structures. Operational offices are situated in Luxembourg, the United Kingdom, and Romania. The jurisdiction overseeing MindGeek's content-related operations is based in Cyprus.

As it was already discussed in this research, it's crucial to understand that the violence and the consequences of these crimes from the victims doesn't end when the videos are deleted as not even a successful suit can avoid the spread of an image that was already spread (Franks et al, 2014) — Victims still lose their jobs, have their reputations ruined and live with fear. The role of legislations here is to protect not only the digital identity and personality of the victims, but also bring justice to something that used to feel impossible as the tracking methods are improving.

In 2018 the Brazilian Criminal Code, more specifically the article 216-B,

[95]Available here: https://businessinthenews.co.uk/2020/07/19/pornhub-receives-more-website-traffic-than-amazon-and-netflix-new-research-reveals/

regulated the Non-Consensual Pornography crime: "To produce, photograph, film, or record, by any means, content featuring scenes of nudity or sexual or lewd acts of an intimate and private nature without the participants' authorization. Penalty - imprisonment, from 6 (six) months to 1 (one) year, and a fine. Sole Paragraph. The same penalty applies to anyone who creates a montage in a photograph, video, audio, or any other recording with the purpose of including a person in scenes of nudity or sexual or lewd acts of an intimate nature."

This article came to fill a gap regarding the punishment for the conduct of individuals who recorded the practice of sexual acts between third parties in private environments is filled. This pertains to the practice known as voyeurism. Although it was a conduct that seriously violated privacy and could already give rise to compensation for moral damages, the act of someone, for instance, installing recording equipment on the premises of a property to capture intimate images without the consent of the occupants did not fall within any criminal offense. This article is related to the General Data Protection Law (LGPD) in the context of the right to privacy and protection of personal data. Although it does not directly address issues related to the protection of personal data, it connects with the LGPD in the sense of safeguarding the privacy and intimacy of the individuals involved. By capturing or recording scenes of nudity or sexual acts without the participants' authorization, Article 216-B aims to protect the intimate sphere of the individuals involved. The LGPD, in turn, seeks to ensure the protection of personal data, ensuring that the processing of such information is carried out appropriately, transparently, and respecting the rights of data subjects, including the right to privacy.[96]

Therefore, while Article 216-B of the Penal Code focuses on the protection of privacy in specific situations, the LGPD has a broader scope, addressing the processing of personal data in various situations, both online and offline. Both legislations share the common goal of safeguarding fundamental rights related to the intimacy and privacy of individuals.[97]

---

[96] Mariana Nascimento Maia and Rafael Baioni Do Nascimento, "Pornografia de Vingança no Ordenamento Jurídico-Penal Brasileiro" *Confluências | Revista Interdisciplinar de Sociologia e Direito* 24, no. 2 (August 1, 2022): 104–25, doi:10.22409/conflu.v24i2.53554.

[97] Gabriela Soldano Garcez and Izabela Clementino De Miranda Gonçalves, "Obstáculos Na Proteção Do Direito À Privacidade E Da Honra Da Mulher Na Internet," *LEOPOLDIANUM* 49, no. 138 (September 1, 2023): 16, doi:10.58422/releo2023.e1419.

Now bringing the General Data Protection Regulation to the discussion in a comparative manner, it is important to note that as it comes from a regulation that should be applied to more than one country (as this regulation is used in the members of the European Union) it is understandable that it won't be directly specified as a crime, because we are not analyzing particular national regulations. In 2018, the implementation of the GDPR provided a regulatory avenue for addressing potential undesired disclosures, although its effectiveness in fully safeguarding individuals from such incidents remains uncertain.

As already discussed in this research, the number of cases of Non-Consensual Pornography didn't stop growing as a pandemic of cyber-violence. Not only governments started to create their own programs in order to address, track and hold accountable the perpetrators of those crimes.: one of the most notable organizations dedicated to combatting Non-Consensual Pornography worldwide is managed by South West Grid for Learning (SWGfL) and it's called StopNCII.org that is an international leg of the Revenge Porn Helpline from the UK. It was launched in December 2021, during its first year, the organization has seen over fourteen thousand cases and created over fifty thousand hashes to help victims with Non-Consensual Pornography (Non-Consensual Pornography) reports. [98]

In Europe, the Cyber Rights Organization[99] has the main mission of entail the elimination of every online threat which may deprive an individual from a safe and secure use of the Web. It offers assistance to victims on how to pursue their rights and delete their data that was leaked. The European Union is still discussing the creation of a regulation that would turn Non-Consensual Pornography a criminal offense across the bloc. In 2022 the European Commission presented a proposal pushing the members to implement tougher rules to combat violence against women. But the block was divided, and the draft law was rejected in 2023 which means that there's no consensus between the members regarding this crime.[100] However, It is worth mentioning some particular legislations of a few nations as a matter of comparison.

[98] Information taken from the Revenge Porn Helpline Report of 2022 available here: https://revengepornhelpline.org.uk/assets/documents/rph-report-2022.pdf?_=1681885542

[99] https://cyberights.org/

[100] Available here: https://www.politico.eu/article/rape-europe-criminal-offense-non-consensual-sex/

England and Wales disposed on the Criminal Justice and Courts Act of 2015, article 33:[101] “It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made: without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress.” There are some exceptions on subparagraphs of the article, if the disclosure was made to the depicted person and if the defense prove that the disclosure was necessary for a crime prevention, for journalistic purposes in the public interest, or if the material was previously disclosed for reward with no reason to believe it lacked consent. The accused bears the burden of proof for defenses, and penalties range from fines to imprisonment.

Scotland disposed on the Abusive Behaviour and Sexual Harm Act of 2016, article 2[102]: “A person (“A”) commits an offense if A discloses, or threatens to disclose, a photograph or film which shows, or appears to show, another person (“B”) in an intimate situation, by doing so, A intends to cause B fear, alarm or distress or A is reckless as to whether B will be caused fear, alarm or distress, and the photograph or film has not previously been disclosed to the public at large, or any section of the public, by B or with B’s consent.”. The accused has defenses, such as the person's consent or a reasonable belief in consent. Penalties include up to 12 months imprisonment or a fine on summary conviction, and up to 5 years imprisonment or a fine on conviction on indictment.

Northern Ireland disposed on the Justice Act of 2016, article 51:[103] “It is an offense for a person to disclose a private sexual photograph or film if the disclosure is made without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress.”. Penalties range from imprisonment up to 2 years or a fine on indictment, and imprisonment up to 6 months or a fine on summary conviction. Schedule 4 addresses special provisions for those providing information society services.

Spain also criminalizes Non-Consensual Pornography in its Criminal Code on article 197.7:[104] “Whoever, without the authorization of the affected party, discloses,

[101] Avalable here: https://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted?view=plain
[102] Available here: https://www.legislation.gov.uk/asp/2016/22/section/2/enacted?view=plain
[103] Available here: https://www.legislation.gov.uk/nia/2016/21/section/51/enacted?view=plain
[104] Boletín Oficial del Estado. "Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal." Accessed January 25, 2024. https://www.boe.es/eli/es/lo/1995/11/23/10/con.

communicates or reveals images or audiovisual recordings to third parties, obtained with the affected party's consent in a private residence or at any other location out of the sight of third parties, if said disclosure seriously damages the personal privacy of the individual, shall be punished with a prison sentence of three months to one year or a fine of six to twelve months." — Beyond the dedicated provision in its Penal Code, Spain's Organic Law 15/1999 on the Protection of Personal Data empowers individuals to request the removal of inappropriate or excessive intimate content from websites. The Spanish Agency of Data Protection possesses the authority to expunge data upon request, and it is also empowered to demand the removal of content from European websites while having the capability to restrict access to specific content within Spain.

The roles of Legislations are clear when it comes to Non-Consensual Pornography. Creating a safe space online is a matter of interest to everyone that is present on the online world, but more than safe, the punishments for those crimes should be ideally standardized, not only in a Civil manner with fines and removal of contents, but also with criminal penalties defined in a uniform manner. The social factor is also a heavy burden to carry, as many women can be reluctant to report incidents due to fear of retaliation, social stigma or concerns about the privacy implications of pursing legal actions. [105]

The modifications in laws and policies across various levels would ideally highlight the importance of adopting a comprehensive approach to tackle this problem. However, a critical concern revolves around the persistent presence of sexually explicit or intimate images in cyberspace after distribution, exacerbated by the limited impact of existing laws on content removal. This is particularly evident as many hosting sites for such images operate outside the jurisdiction of the victim's country. Even when specific laws are in place, holding someone accountable when they could be located in other jurisdictions or even when it is not possible to locate the perpetrators. The widespread practice of reblogging and reposting on the Internet further complicates the issue, making it challenging or even impossible to retract the disseminated images.[106]

---

[105] Simon Jones, "Revenge Porn Victims Suffering in Silence - Survey Shows Law Not Fit for Purpose and Needs to Change," *Police, Fire and Crime Commissioner North Yorkshire*, November 20, 2018, https://www.northyorkshire-pfcc.gov.uk/news/revenge-porn-victims-suffering-in-silence-survey-shows-law-not-fit-for-purpose-and-needs-to-change/.

[106] Nicola Henry and Anastasia Powell, "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law," *Social & Legal Studies* 25, no. 4 (2016): 397–418, doi:10.1177/0964663915624273.

3.2. Potential Solution in Combatting Non-Consensual Pornography: Copyright and the Right to Be Forgotten

If this research has the main goal of serving as an information point and refuge for victims, there's nothing more fair than exploring possible solutions to combat and fight Non-Consensual Pornography. One of the main findings of a study made in the United Kingdom was that the harms caused by this violence were constant, and since the spread was not under the victim's control they had a sense of living constantly threatened by the possibility of those emerging once again. One of the victims said: "[It's] having this continuing threat that the images could be re-shared, or re-emerge online, that new people could see these intimate images. And I think it's the unknowing; that not knowing aspect that you have to deal with every day."[107].

The harms caused by Non-Consensual Pornography are continuous and terrifying for the victims, however, some legal frameworks can be used to stop this content from spreading and trying to delete it from the Internet. When Non-Consensual Pornography and technology-facilitated crimes were not even a possibility, Copyright regulation was under discussion in England, even though not regarding specifically pornography, but regarding the rights of publishing exclusive stories and books. Before 1695 there was a publishing monopoly in place in England, it was controlled by the Stationers' Company with the blessing of the crown. In 1970 the Act of Anne, a regulation that brought for the first time a system where authors had exclusive rights to their works for a specific period; with this, only the author (or those who were authorized by the author) could print, publish and sell their work for a period. After the time was over, the work became public domain and the general public could use it. [108]

Copyright regulation stemming from the Act of Anne[109], began to emerge in various countries, such as the United States in 1790. But international coordination regarding copyright was lacking until the 19th century. In 1886, the Berne Convention was established to facilitate reciprocal acknowledgment of copyright among nation-states and foster the establishment of global standards for copyright protection. It

[107] Clare McGlynn et al., "'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse," *Social & Legal Studies* 30, no. 4 (2021): 541–62, doi:10.1177/0964663920947791.

[108] Julio Carvalho, *A Cultural History of Copyright: From Books to Networks* (Cham: Springer Nature Switzerland, 2023), doi:10.1007/978-3-031-46854-4.

[109] Available here: https://www.legislation.gov.uk/aep/Ann/6/8

obviated the necessity for separate registration of works in each individual country and has gained near-universal adoption, encompassing 181 out of the 244 states and territories. A significant transformation brought about by the Convention was the extension of copyright protection to unpublished works, eliminating the need for registration; this implies that individuals (or their affiliated organizations) automatically hold copyright over any work once it is recorded, whether through writing, drawing, filming, or other means.[110]

With time, realities, necessities and technology, the need for a specific law took place and in 1988 the Copyright, Designs and Patents Act was put into place (CDPA). And according to this regulation on the article 1, b, Copyright is: "A property right which subsists in accordance with this Part in the following descriptions of work, sound recordings, films or broadcasts"[111]. It is inherently established upon the creation of a work and does not necessitate formal registration as it is regulated on the section 11 of the CDPA: "The author of a work is the first owner of any copyright in it, subject to the following provisions." It affords the author exclusive entitlements, encompassing control over aspects such as distribution, reproduction, and public accessibility of the work.[112]

Bringing this concept to such a situation where a picture, video or private conversations are leaked, the copyright owner of the content possesses the authority to demand that a website abstain from disseminating or replicating the image. In instances where they own the copyright to an image, seeking cooperation from the uploader becomes unnecessary. Rather, their copyright grants them the exclusive prerogative to oversee the distribution and reproduction of the image, enabling them to utilize this right to impede further dissemination by a website.[113]

, where the author of the photo is also the subject, or when pictures were captured by the victims themselves, automatic ownership of copyright ensues. Conversely, if the photograph is taken by someone else, that individual assumes the role of the copyright owner. Similarly, in cases involving digitally manipulated Personal

[110] "Copyright History | Intellectual Property Rights Office," accessed January 20, 2024, https://intellectualpropertyrightsoffice.org/copyright_history/?v=99ED03F0-D0D6-4406-B94E-548067279E51.

[111] Available here: https://www.legislation.gov.uk/ukpga/1988/48/section/1?view=plain

[112] https://www.legislation.gov.uk/ukpga/1988/48/section/11

[113] Aislinn O'Connell and Ksenia Bakina, "Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal," *Legal Studies* 40, no. 3 (2020): 442–57, doi:10.1017/lst.2020.17.

Sexual Imagery (PSI), such as superimposing faces, the copyright ownership belongs to the creator of that work, not the person depicted.[114] However, if the subject of an image or video was unaware of being recorded or photographed, or had no involvement in the recording or photography, as is often the case in videos depicting rape or assault, or covertly captured images, they are precluded from asserting any claim to copyright. Consequently, they are unable to leverage copyright protection to exert control over the use of their image.

Regarding the platforms where those contents can be shared and spread, the United States have a way more structured regulation, it is called the OCILLA (Online Copyright Infringement Liability Limitation Act), and on the article 512, C it says: "A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider— **(i)** does not have actual knowledge that the material or an activity using the material on the system or network is infringing; **(ii)** in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or **(iii)** upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;" [115]

So, if victims sees their picture or video in a platform, they could use the "notice and takedown" mechanism and in order to avoid eventual lawsuits for infringement of copyright, once the website has received notification that the image is infringing and should be taken down, it is required to comply. Thus, a content owner may send a notification to a website which is hosting a non-consensual or abusive image (notice), and the website should remove it within a relatively short space of time (takedown). There is no specific time limit on takedown, but the Act provides that the service provider must respond 'expeditiously to remove, or disable access, to the material'.[116] This would represent a fast and cheap solution, as it wouldn't need a lawyer for representation.

---

[114] Idem.

[115] Available here: https://www.govinfo.gov/content/pkg/USCODE-2022-title17/html/USCODE-2022-title17-chap5-sec512.htm

[116] Aislinn O'Connell and Ksenia Bakina, "Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal," *Legal Studies* 40, no. 3 (2020): 442–57, doi:10.1017/lst.2020.17.

The EU has a similar system, it is disposed on the article 14 of the E-Commerce Directive: “Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.”[117]

In this Directive, it is not clear how the victim should fill the report and request the removal of the content. However, the Intellectual Property Crime Project (IPC) elaborated a step-by-step procedure, that is basically the same as the one used in the United States. A notice should be made containing the following requirements: The copyright holder details, a detailed description of copyright-protected material (name, type of content and any relevant information), where the content is located and your contact information.[118]

While notice and takedown is not flawless, it remains a valuable tool in addressing Non-Consensual Pornography for the victims. Despite its limitations, it proves effective, especially on larger platforms like social media and legitimate adult content sites. However, challenges still persist, as issuing takedown notices doesn't prevent image re-upload on other sites. Legal action for non-compliant websites is costly and impractical for multiple requests, potentially hindering victims' access to justice and protection of their rights[119].

To exercise the right to be forgotten, an individual must notify the data controller (the entity responsible for processing your personal data. In the context of an online picture, it could be the website owner, the photographer, or the platform hosting the image) about non-consensual data listings. Once a request for the removal of personal data is made, the data controller or search engine is obligated to take

[117] Available here: https://eur-lex.europa.eu/eli/dir/2000/31/oj

[118] “Copyright Infringement Notice | Eurojust | European Union Agency for Criminal Justice Cooperation,” accessed January 20, 2024, https://www.eurojust.europa.eu/publication/copyright-infringement-notice.

[119] Amanda Levendowski, “Using Copyright to Combat Revenge Porn,” *NYU Journal of Intellectual Property & Entertainment Law*, May 1, 2014, https://jipel.law.nyu.edu/vol-3-no-2-6-levendowski/.

appropriate action. This right places a significant burden on data controllers to assess whether a takedown request based on this right should be accepted.[120] If unsuccessful, file a complaint with the relevant Data Protection Authority (The Data Protection Authority (DPA) is the regulatory body responsible for enforcing data protection laws on the jurisdiction of the victim).

The pervasive dissemination of Non-Consensual Pornography, affecting diverse women on a global scale, underscores the urgency of understanding user behaviors on social media platforms. Consequently, the analysis and collection of pertinent data should assume critical significance in this regard. In a report published in July 2023, the global population has reached 8.05 billion, showing a growth of just under 1 percent compared to the previous year, with an increase of 70 million people. In terms of technology adoption, there are 5.56 billion unique mobile subscribers worldwide, constituting 69.1 percent of the global population. The mobile phone users increased by 2.7 percent over the past year, with nearly 150 million new users. A growth of 2.1 percent on the internet users was noticed since July 2022, reaching 5.19 billion in July 2023, which accounts for 64.5 percent of the world's population. [121]

Social media usage has seen a 3.7 percent increase since the previous year, with the number of active social media users reaching 4.88 billion, equivalent to 60.6 percent of the world's population. This growth is attributed to the addition of 173 million new active social media identities.[122]

But what does that mean, and how is this connected to the offense that is being discussed in this research? The answer is simple, while there are some cases and contents that are shared through other platforms, such as porn websites, by text and even in person, the majority of the cases and occurrences are shared on social media platforms, making them visible to the victim's friends and family.[123]

---

[120] Aseri, Ankita. 2020. “Juxtaposing Right to Be Forgotten and Copyright Law”. *Journal of Intellectual Property Rights* 25 (3&4):100-104. https://ischolar.sscldl.in/index.php/JInctlPR/article/view/203710.

[121] “Digital 2023 July Global Statshot Report,” *DataReportal – Global Digital Insights*, July 20, 2023, https://datareportal.com/reports/digital-2023-july-global-statshot.

[122] “Digital 2023 July Global Statshot Report.”

[123] Cecilia Grimaldi, “A Post for Change: Social Media and the Unethical Dissemination of Nonconsensual Pornography,” *UC Law SF Communications and Entertainment Journal* 43, no. 1 (January 1, 2021): 109, https://repository.uclawsf.edu/hastings_comm_ent_law_journal/vol43/iss1/5.

Digital platforms like Facebook (now called META) and Telegram play big roles in how we communicate online. They both aim to connect people, but they do it in different ways. META, through Facebook, is like a giant in the social media world, influencing how people interact globally. By looking at META's rules, like those dealing with sexual exploitation of adults, we get to understand how they try to make the online space safe.

On the other hand, Telegram stands out for putting a lot of importance on user privacy and freedom. The platform's strong commitment to keeping conversations private and protecting user data makes it attractive to those who want more confidential communication. As we explore these platforms, it's crucial to dig into their rules, features, and main ideas. This helps us understand the many sides of today's digital communication and how it affects the way we connect and talk online.

Since 2017, Facebook has consistently updated its policies, including data policies, terms of service, and community standards, to respond to and address Involuntary Pornography and other technology-facilitated offenses. The platform explicitly prohibits the sharing or threats to share content related to "sextortion," "revenge porn" or "non-consensual intimate images," and "upskirts". The prohibition on "non-consensual sharing of intimate images" is based on three criteria: the content being "non-commercial" or created in a private setting, the individual depicted engaging in sexually explicit acts or poses, and a lack of consent indicated by a "vengeful context" (e.g., captions, comments, page titles), independent sources, or victim allegations. [124]

Telegram, on the other hand, only considers removal requests for "illegal pornographic content" shared on publicly accessible channels or bots. Users can invoke the Right of Erasure (Right to Be Forgotten) under GDPR, but this only applies to data within their access. For personal data shared privately between users, including non-consensual private information, victims cannot request the erasure. [125]

Although it’s not possible to stop and guarantee completely the spreading of personal information and data without consent, both frameworks can be considered a

[124]Facebook. "Community Standards: Sexual Exploitation of Adults." Transparency, Facebook, https://transparency.fb.com/en-gb/policies/community-standards/sexual-exploitation-adults/. Accessed January 24, 2024.

[125]“Telegram Privacy Policy,” *Telegram*, accessed January 24, 2024, https://telegram.org/privacy.

tool to address and delete content from certain social media or search engines, while those can use tools and even Artificial Intelligence to locate the footprints of the data and delete from more places.

3.3. The use of tools and AI to trace and delete pictures online by platforms

This research should encompass not only regulatory interventions, but also practical and technical remedies addressing Non-Consensual Pornography.

In order to address the use of social media platforms to disseminate illegal content, companies saw the need to create new tools to track criminal activities and non-consensual content. Some new — and controversial — technologies can also be used to predict crimes based on patterns and behavior online. As crime data becomes more accessible and technology progresses, researchers allegedly have a chance to explore crime detection using machine learning and deep learning methods. Machine learning involves using statistical models and algorithms to analyze data and make predictions, while deep learning employs artificial neural networks with multiple layers to model intricate relationships between inputs and outputs. Both machine learning and deep learning offer various applications for crime prediction, but it holds criticism from different scholars.[126]

It is paramount to understand beforehand that crime is a complex antisocial phenomenon that has grown in scale over time[127], and the criticism regarding machine learning technologies and crime prevention using those tools is that algorithms cannot fully predict human behavior. Not only that, but while this can sound as an improvement of the technology, in reality it has been proved that this type of crime prediction causes more harm than solutions in real life. Machine learning models can inherit biases from the data they are trained on historical data used to train these models

[126] Varun Mandalapu et al., "Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions," *IEEE Access* 11 (2023): 60153–70, doi:10.1109/ACCESS.2023.3286344.

[127] Robinson Umeike, "Comparative Crime Analysis and Prediction Using Machine Learning Algorithms: Assessing the Tools and Addressing the Threats," in *2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI)* (2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI), Atlanta, GA, USA: IEEE, 2023), 135–42, doi:10.1109/ICTAI59109.2023.00027.

inherently contain biases, such as racial profiling or socioeconomic disparities, so that the algorithms may perpetuate and even exacerbate those. [128]

Relying solely on machine learning algorithms for crime prevention may overlook the importance of human judgment, contextual understanding, and community involvement in addressing complex social issues related to crime. It's essential to complement technological solutions with human expertise and community engagement to develop holistic approaches to crime prevention. According to the authors, the creators of those machine learning technologies can "confuse correlation with causation. They back up their analysis with reams of statistics, which give them the studied air of enhanced science." Which is not reliable enough when it may affect a whole group of minorities in the meanwhile.[129]

When it comes to tracking images and transforming them into data, the first software created with this intention was called PhotoDNA[130], by Microsoft in a partnership with Dartmouth College, which generates a distinctive digital signature, referred to as a "hash" for an image. This hash is subsequently compared to the signatures of other photos to identify copies of the same image. When integrated with a database containing hashes of previously identified illegal images, it becomes a powerful tool for detecting, disrupting, and reporting the distribution of child exploitation material.

Microsoft contributed PhotoDNA to the National Center for Missing & Exploited Children (NCMEC), which serves as the central hub and extensive reporting facility in the United States for matters related to preventing and addressing child victimization, including abduction, abuse, and exploitation. The CyberTipline, operated by NCMEC, offers the public and electronic service providers (ESPs) a platform to report cases of online enticement of children for sexual acts and the dissemination of child exploitation material. Microsoft continues to offer this technology without charge to qualified organizations, including technology companies, developers, and non-profit

[128] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, First edition (New York: Crown, 2016).
[129] O'Neil, *Weapons of Math Destruction*.
[130] "PhotoDNA | Microsoft," accessed January 30, 2024, https://www.microsoft.com/en-us/photodna.

entities, in the ongoing effort to combat child exploitation.[131] Free access to PhotoDNA has also been extended to law enforcement, primarily through forensic tool developers.[132] This technology has been widely integrated into advanced visual image and forensic tools utilized by law enforcement agencies worldwide as it seems to be a useful tool that can be adapted and used in different scenarios. In 2015, Microsoft made PhotoDNA available as a service on Azure, an advanced content moderation platform, it integrates seamlessly with the PhotoDNA Cloud Service. This integration enhances the capabilities of smaller companies and organizations by not only permitting users to upload content, but also ensuring the integrity of their platforms. The combined solution utilizes AI models to swiftly detect offensive or inappropriate content in both text and images, in order to create a safer and more reliable online experience for all users.

A bit ahead, in 2017, when Facebook saw that technology facilitated crimes occurrences were happening in their platform, they expressed their first interest in making the website a place where people would find entertainment and not be afraid of finding or being exposed without their consent. They launched a pilot plan in Australia in partnership with the Australian eSafety Commissioner's Office and a specific group of victims and advocates, concerned about explicit images being exposed and shared without consent. The pilot plan consisted in a voluntary program to avoid the wide spreading of content, and it should work in a simple way. Basically, the victim should complete an online form on the eSafety Commissioner's official website and submit the image via Messenger, then the office will notify Facebook without accessing the images. Upon receiving the notification, a specially trained representative from the Community Operations team reviews and hashes the image, creating a human-unreadable numerical fingerprint (similar to the technology used by PhotoDNA explained previously). Facebook would store the photo hash — not the photo — to prevent future uploads. If someone attempts to upload the image, it is checked against the database of these hashes; if a match is found, posting or sharing is prohibited. After

[131] "PhotoDNA Cloud Service | Microsoft," accessed January 21, 2024, https://www.microsoft.com/en-us/photodna/cloudservice.

[132] "Since its inception, PhotoDNA technology has been widely adopted into innovative visual image and forensic tools exceptionally used by law enforcement today. These tools range from free forensic and image review tools to large scale law enforcement platforms used by entire countries on server platforms. This is great news for law enforcement, as they no longer need to take raw code and hire IT staff to work the code into a tool or platform. As a result, law enforcement should ask their current tool providers if they are using PhotoDNA technology. If not, they can contact pdnarequests@microsoft.com to start the PhotoDNA on-premise licensing procedures." — "PhotoDNA FAQ | Microsoft," accessed January 21, 2024, https://www.microsoft.com/en-us/photodna/faq.

hashing the photo, the company would inform the reporter via their provided secure email, asking them to delete the photo from the Messenger thread; upon confirmation, we delete the image from our servers.[133] This raised a lot of different opinions saying that the company was asking victims to send them the private content so they could stop Non-Consensual Pornography.[134]

As the program was not received in good terms by the users that were afraid that employees would have access to the pictures, prolonging the harms and the unsafe feeling on the victims, in March 2019 Meta launched its own Artificial Intelligence to find this type of content in a faster way to support the victims more effectively. The difference here was that Meta could now detect contents even before the victim reports them to the platform. And this was theoretically crucial to interrupt the continuum violence caused by Non-Consensual Pornography and previously discussed here in this research. The procedure here would be that a proficient member of the Community Operations team, specifically trained for this role, will systematically examine the content identified by the AI and if that image or video is determined to contravene what is described in the Community Standards[135], it will be automatically detected, accompanied by the disabling of the associated account, particularly in cases involving the unauthorized dissemination of intimate content.[136]

The NCII Pilot was deactivated in 2021[137], and it was integrated to StopNCII.org, a free platform that used technology to prevent the sharing or resharing of intimate images. With partnerships with big social media platforms, such as Facebook, TikTok, Reddit, Bumble, OnlyFans, Threads, Instagram and Snap Inc, the organization can reach and send reports with a bigger range and faster results.

This institution was mentioned here before, in section 3.1, it is operated by the Revenge Porn Helpline (that is part of SWGfL — South West Grid for Learning[138]).

---

[133] "The Facts: Non-Consensual Intimate Image Pilot," *Meta*, November 9, 2017, https://about.fb.com/news/h/non-consensual-intimate-image-pilot-the-facts/.

[134] "Facebook: Send Us Your Naked Photos to Stop Revenge Porn - CBS News," May 24, 2018, https://www.cbsnews.com/news/facebook-revenge-porn-naked-photos-pilot-progam/.

[135] Facebook. "Sexual Exploitation of Adults." Facebook Community Standards. Accessed January 21, 2024. https://transparency.fb.com/en-gb/policies/community-standards/sexual-exploitation-adults/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fsexual_exploitation_adults

[136] "Detecting Non-Consensual Intimate Images and Supporting Victims," *Meta*, March 15, 2019, https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/.

[137] https://about.meta.com/actions/safety/topics/bullying-harassment/ncii/pilot

[138] "Safety and Security Online | SWGfL," accessed January 30, 2024, https://swgfl.org.uk/.

They also operate in Brazil, in partnership with the SaferNet organization[139]. The Brazilian partnership offers an anonymous reporting service for crimes and Human Rights violations on the Internet. It has established collaborations with government entities, private sector partners, and law enforcement, fostering cooperation with judicial authorities.

Even with the program discontinued, Meta continues with their attempts to improve, protect and block this kind of content. The process of reporting is detailed in their website, and it varies depending on the platform (Instagram[140], Facebook[141] or Messenger[142]), according to them, the team reviews the content reported in more than 70 languages, and they operate continuously, seven days a week, throughout the entirety of a 24-hour cycle to ensure the coverage and the fastest assistance possible to the victim.

On the other hand, when it comes to machine and deep learning, studies that support and believe in this technology explain that[143], the initial phase involves gathering pertinent data, encompassing crime statistics, demographics, and meteorological patterns. Subsequently, the data undergoes preprocessing, entailing cleaning and formatting it into a usable structure. Following preprocessing, the data is partitioned into training and testing sets for model development and assessment. Feature engineering ensues, entailing the identification of pertinent data attributes conducive to model training. Upon feature selection, a range of machines and deep learning algorithms can be applied to the data for training and prediction tasks. Ultimately, the trained models undergo evaluation using diverse performance metrics to gauge their accuracy and efficacy in crime prediction. The outcomes gleaned can inform decision-making within law enforcement and crime prevention endeavors, which the main criticism regarding these technologies, as attested in previous paragraphs, those

[139] https://new.safernet.org.br

[140] "Privacy and Safety Center." Instagram Help Center. Accessed January 30, 2024. https://help.instagram.com/165828726894770?ref=ig_about

[141] "Report Content on Facebook." Facebook Help Center. Accessed January 30, 2024. https://www.facebook.com/help/1380418588640631

[142] "Reporting Conversations" Facebook Help Center. Accessed January 30, 2024. https://www.facebook.com/help/messenger-app/1165699260192280/

[143] Neil Shah, Nandish Bhagat, and Manan Shah, "Crime Forecasting: A Machine Learning and Computer Vision Approach to Crime Prediction and Prevention," *Visual Computing for Industry, Biomedicine, and Art* 4, no. 1 (April 29, 2021): 9, doi:10.1186/s42492-021-00075-z.

Mandalapu et al., "Crime Prediction Using Machine Learning and Deep Learning."

Sapna Singh Kshatri et al., "An Empirical Analysis of Machine Learning Algorithms for Crime Prediction Using Stacked Generalization: An Ensemble Approach," *IEEE Access* 9 (2021): 67488–500, doi:10.1109/ACCESS.2021.3075140.

software programs and machines hold with them biases and concepts that can create mass incarceration and maintain inequalities installed and rooted in our civil society. [144]

Despite these ethical concerns, the question whether these kind of technologies would help the victims as a preventive tool to predict the offenses still remains In theory, the machines can "learn" and "understand" how the violence cycle works and the machine could stay in alert mode in order to monitor and even avoid the upload of the eventual pictures, videos or contents in general when facing some behavior recognized as suspicious. A study made in 2022 to see if the machines could identify offenders, utilizing different machine learning techniques, to evaluate cybercrime detection methods. One of the results was that a specific method exhibited the highest performance in identifying cybercriminals, achieving a remarkable accuracy rate of 96.56%. The research underscores the efficacy of employing sophisticated machine learning algorithms in enhancing network security and cybercrime detection capabilities. Through real-time data analysis and cluster computing techniques, the study demonstrates the feasibility of accurately identifying artificially created cybercrime instances.[145]

While the potential of AI in enhancing cybercrime detection capabilities is evident, it's crucial to approach its application with caution and a critical mindset regarding its trustworthiness. Firstly, as mentioned before, systems are not infallible and can be prone to biases present in the data they are trained on. In the context of cybercrime detection, biases in training data can lead to erroneous identifications or even discriminatory outcomes, especially when dealing with sensitive matters such as criminal behavior. Secondly, the high accuracy rate mentioned in previous studies may not translate perfectly into real-world scenarios. The performance of AI models can vary significantly depending on factors like the diversity of data, the evolution of cyber threats, and the adaptability of criminals to circumvent detection methods. Furthermore, relying solely on AI for cybercrime detection raises ethical concerns regarding privacy and surveillance. The idea of constant monitoring by machines to preemptively identify potential offenders may infringe upon individuals' rights to privacy and due process.

[144] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, First edition (New York: Crown, 2016).

[145] K. Veena et al., "Cybercrime: Identification and Prediction Using Machine Learning Techniques," ed. Dalin Zhang, *Computational Intelligence and Neuroscience* 2022 (August 27, 2022): 1–10, doi:10.1155/2022/8237421.

Nonetheless, it is important not to disregard the significance of automation in criminal justice settings. Automation has the potential to augment understanding of the criminal justice system. Should a particular judicial procedure exhibit tendencies towards discriminatory or arbitrary outcomes, the integration of automated tools could potentially enhance the administration of justice.[146]

It's important to recognize that while AI can be a valuable tool in combating cybercrime, it should be complemented with human oversight, ethical considerations, and legal frameworks to ensure accountability and fairness in its use. Trust in AI systems should be built through transparent practices, robust validation processes, and ongoing scrutiny of their performance and impact on society.[147]

In order to use technology on the victim's side, scholars have been evaluating the possibility of creating a system that helps to prevent the sharing of pictures without the sender's consent. Not involving machines and AI in some kind of value, ethical or moral decision, just mechanically impeding them to record, share and forward content without consent.[148] More or less like the technology used by Disney+, Netflix and Amazon Prime that works like this: when users try to record the screen while watching a movie or a series through their phones or computers, they see a black screen as the content is protected by the Digital Rights Management (DRM)[149].

Some recent cases are important to be mentioned here to understand the functioning of the detection software programs used by platforms and how they can be misled. In 2019 Katie Hill became a victim when private pictures of her were leaked without her consent, which caused her voluntary resignation of her public role at the United States Congress. The gap here was that one newspaper that published the picture did not post directly on Facebook, they used their external website to upload the illegal

[146] Aleš Završnik, "Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings," *European Journal of Criminology* 18, no. 5 (2021): 623–42, doi:10.1177/1477370819876762.

[147] Tobias M. Peters and Roel W. Visser, "The Importance of Distrust in AI," in *Explainable Artificial Intelligence*, ed. Luca Longo, vol. 1903 (Cham: Springer Nature Switzerland, 2023), 301–17, doi:10.1007/978-3-031-44070-0_15.

[148] Mirko Franco, Ombretta Gaggi, and Claudio E. Palazzi, "Can Messaging Applications Prevent Sexting Abuse? A Technology Analysis," *IEEE Transactions on Mobile Computing*, 2023, 1–14, doi:10.1109/TMC.2023.3238189.

[149] Amir Rafi, Carlton Shepherd, and Konstantinos Markantonakis, "A First Look at Digital Rights Management Systems for Secure Mobile Content Delivery," 2023, doi:10.48550/ARXIV.2308.00437.

content and after shared as a link on Facebook turning the pictures undetectable by the platform, but still using it to disseminate that private content. [150]

A second newspaper used a different approach, for its initial story about Hill, the platform opted for the same image across Twitter, Facebook, and search engine results: a collage comprising four distinct photos of Hill. The primary photo, cropped, seemingly portrays her unclothed, mirroring the initial image seen in the story itself — Both behaviors are against the Terms of Use determined by Facebook as explained in the previous section and when they noticed it, the contents were deleted from the platform, but only after thousands of users already shared the story and the link that contained the pictures on the thumbnail, reaffirming here the importance of time, and human swift review of cases to erasure contents on social media. [151]

Another crucial aspect employed to safeguard victims and mitigate occurrences involves raising awareness and promoting proactive measures. Since 2019 Meta declared to be interested in maintaining their platforms as safe as possible, so more than improving their policies, creating artificial intelligence programs to delete private content shared without consent, they are determined to strengthening efforts against the dissemination of non-consensual intimate images.[152] Facebook has streamlined its reporting mechanisms, making it easier for users to flag and report instances of non-consensual intimate images. This enhancement aims to empower users to take action against such harmful content swiftly. Collaboration and partnerships play a crucial role in Facebook's efforts to combat the spread of non-consensual intimate images. The company states that they collaborate closely with external organizations and experts in the field to develop effective strategies and initiatives. By pooling resources and expertise, Facebook and its partners strive to create a safer online environment and prevent the dissemination of harmful content.[153]

---

[150] Caitlin Kelly, "Facebook's Anti-Revenge Porn Tools Failed to Protect Katie Hill," *Wired*, accessed January 26, 2024, https://www.wired.com/story/katie-hill-revenge-porn-facebook/.

[151] Jessica Bennett, "The Nudes Aren't Going Away. Katie Hill's OK With That.," *The New York Times*, August 8, 2020, sec. Style, https://www.nytimes.com/2020/08/08/style/katie-hill-she-will-rise-revenge-porn.html.

[152] "Making Facebook a Safer, More Welcoming Place for Women," *Meta*, October 29, 2019, https://about.fb.com/news/2019/10/inside-feed-womens-safety/.

[153] "Strengthening Our Efforts Against the Spread of Non-Consensual Intimate Images," *Meta*, December 2, 2021, https://about.fb.com/news/2021/12/strengthening-efforts-against-spread-of-non-consensual-intimate-images/.

In December 2021, X (formerly known as Twitter) determined that users are not allowed to post or share intimate content that was produced or distributed without consent. The content can be reported by anyone, and the contents that go against the policies of the platform in this sense are basically: Creepshots or upskirts (unauthorized photos taken of individuals without their consent, often focusing on private areas or taken in compromising positions), content offering financial rewards for obtaining non-consensual nude media and the sharing of intimate images or videos accompanied by text expressing desires for harm or revenge towards those depicted, along with providing contact information. The process for reporting these occurrences is easy, the victim can do so directly from the post or via the private information report form, selecting the "an unauthorized photo or video" option. [154] However, this doesn't mean that the platform is safe and safeguarded from these kinds of occurrences. A recent case involving the most famous pop star in the world happened earlier this week, Taylor Swift had sexually explicit deep fake pictures spread on X and Telegram mostly. Before the platform was able to hash and delete the pictures, one of the images already had 47 million views, the solution seen by X was to ban the terms "Taylor Swift", "Taylor Swift AI" and "Taylor AI" so people could not find the content easily, however, the pictures can still be found on the platform. After this episode, senators and influential figures manifested their concern regarding deepfake contents as the number of offenses grew over 550% and 99% of the victims targeted in deep fake pornography are women. [155]

Social media platforms tend to go in the same path, working and modifying their platforms in order to strengthen efforts against the spread of non-consensual intimate images underscores its dedication to fostering a safe and supportive online community. Through enhanced reporting mechanisms, technological tools, victim support initiatives, and collaborative partnerships, platforms tend to facilitate reporting processes, creating the feeling of a safe and protected environment for their users. The partnerships with StopNCII.org that started as a test, now linked with different platforms, from livestream (Discord) to dating apps (Bumble) and acts as a middle field between the companies and the victims, proving resources in an easy and free way with

[154] "X's Non-Consensual Nudity Policy | X Help," accessed January 31, 2024, https://help.twitter.com/en/rules-and-policies/intimate-media.

[155] "2023 State Of Deepfakes: Realities, Threats, And Impact," accessed January 31, 2024, https://www.homesecurityheroes.com/state-of-deepfakes/#key-findings.

a website filled with easy access links and reporting tutorials to make this phase as uncomplicated as it can be in a sensitive moment of exposition.[156]

To use the website and report offenses, StopNCII.org asks you to select the intimate content from your device, upload to their platform to generate the digital fingerprint — the technology created by Microsoft mentioned in the beginning of this topic — and the victim should receive a case number, this digital fingerprint called hash, will be shared with the participating companies for them to locate and delete remaining copies on their database. The organization will periodically continue to look for those hash matches and delete them as they appear. The victims are able to check the progress of their report on the website, which provides them some kind of control back from the narrative.

As elucidated earlier within this section, the use of machine learning, image hashing, and assorted methodologies aimed at safeguarding victims of Non-Consensual Pornography could be construed as either a beneficence to facilitate and provide solutions for the victims at the same time that they can perpetuate diverse forms of violence and biased pre-concepts.

[156] "Resources and Support | StopNCII.Org," accessed January 26, 2024, https://stopncii.org/resources-and-support/.

Conclusion

This research had its main focus on understanding available frameworks and tools to address Non-Consensual Pornography and how to employ them in order to protect victims and give them back the control of the narrative stolen by an unwanted exposition. First, the research stressed how it is crucial to understand that Non-Consensual Pornography has a direct connection with gender-based violence, encompassing harmful and detrimental actions perpetrated against individuals or collectives based on their gender identity. It is a phenomenon that primarily target women and girls, spanning across a spectrum of behaviors ranging from physical and sexual violence in physical settings to digital realms, including online sexual harassment, cyberbullying, doxxing, and the dissemination of manipulated images, such as deepfakes. In the evolving landscape of the digital era, a concerning trend of online gender violence has emerged, exploiting the internet's vast reach to harm and shame women. This exploitation underscores the urgent need to address the complex challenges posed by this phenomenon. The internet, originally celebrated as a platform able for promoting interpersonal connection and civic empowerment, is now cynically weaponized to target and victimize women, signifying a troubling shift in gender-based violence dynamics.[157]

Non-Consensual Pornography cases are a rising issue around the world as the reach of social media and the number of users are increasing day-by-day,[158] and that is the motivation behind this whole research and its findings. Seeing women and girls facing this kind of violation, recognizing the size of the issue and the gaps in regulations represent an important step to take in order to see a broader context and evaluate possible solutions within existing frameworks, tools and comparing data protection regulations of Europe and Brazil.

When we analyze the scale of gender violence in Europe, we can notice an ongoing issue in particular on the basis of the EU Agency for Fundamental Rights (FRA) conducted a comprehensive survey on violence against women at the EU level, gathering data from interviews with 42,000 women across all 28 then EU Member

[157] 'Bodyright - Own Your Body Online | Bodily Integrity | UNFPA', *United Nations Population Fund*, accessed 2 February 2024 https://www.unfpa.org/bodyright/.

[158] "Digital 2023 July Global Statshot Report." — as per n.126.

States. The survey,[159] conducted in 2014, focused on women's experiences of physical and sexual violence, sexual harassment, and stalking both in the past year and since the age of 15. The findings of the survey underscore the pervasive nature and scope of violence against women throughout the EU. According to the data gathered, approximately one in three women reported experiencing some form of physical and/or sexual violence since reaching the age of 15. Moreover, one in ten women reported experiencing some form of sexual violence during the same period, with one in twenty reporting incidents of rape. Furthermore, it revealed that slightly over one in five women reported experiencing physical and/or sexual violence from either a current or previous partner. Additionally, 43% of women reported experiencing psychologically abusive and/or controlling behavior while in a relationship.

Regarding digital forms of harassment, the survey found that between 4-7% of women in the EU-27 reported experiencing cyber harassment in the past 12 months, while between 1-3% reported incidents of cyberstalking during the same period. These findings highlight the need for comprehensive measures to address and mitigate the prevalence of violence against women across the European Union. [160]

We can consider the GDPR a result of historical evolution and necessity of alignment within the European Union, as the member countries had their own privacy and data regulations aligned with the Directive 95/46/EC; however, as this was created before the internet era, in order to provide up-to-date regulations for successful business deals the European Commission saw the need of creating a uniform legislative framework for substituting the directive, so that the General Data Protection regulation was approved in 2016 to fill existing gaps, align data treatment and regain people's trust on the treatment of their data.[161]

Brazil also served as a compelling case study highlighting the urgency and prevalence of gender violence, with statistical evidence indicating that one in three women in the country becomes a victim of such acts.[162] This statistic not only

[159] "Violence against Women: An EU-Wide Survey. Main Results Report," *European Union Agency for Fundamental Rights*, February 3, 2014, http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report.

[160] European Parliament Research Service. "Violence against women in the EU." European Parliament. 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739208/EPRS_BRI%282022%29739208_EN.pdf

[161] Voigt and Von Dem Bussche, *The EU General Data Protection Regulation (GDPR)* — as per n. 70.

[162] Visível e Invisível: A Vitimização de Mulheres no Brasil. — as per n. 43

underscores the magnitude of the issue, but also underscores its systemic nature within Brazilian society. The transition of gender violence from a private matter to a critical public health concern underscores its profound societal impact, extending beyond individual relationships to affect the overall well-being of the populace.[163]

Despite concerted efforts to address gender violence in Brazil through the formulation of plans, agreements, and services, the persistent emergence of these initiatives suggests an ongoing struggle. This persistence signals potential shortcomings in the comprehensiveness of existing measures; the imperative for sustained discussions regarding the establishment of support networks reflects a recognition of the gaps in current response mechanisms. The overarching objective transcends merely addressing the aftermath of gender violence; it involves proactively establishing structures to prevent its occurrence and to provide necessary care and protection to those at risk or affected.

One of the main points brought by this research was the discussion and alignment of those regulations to the Valid Consent concept. This is directly connected to Non-Consensual Pornography, as the notion of consent hinges upon the capacity of an individual to take an informed decision. When individuals lack the possibility to comprehend or are unaware of the nature of what they are consenting to, their consent is deemed invalid since it must be offered voluntarily and without coercion. Central to the validity of consent is the principle of comprehension, which presupposes that the consenting party possesses adequate information, and that the act of consenting is a deliberate and intentional choice.[164]The absence of consent and the subsequent exposure represent primary factors that render Non-Consensual Pornography highly distressing for victims, as it deprives them of control over their own narrative.

Under this respect, the research highlighted disparities between the GDPR and LGPD regulations concerning the obligations of data controllers towards the data subjects. The GDPR mandates prompt response to requests for erasure within one month, extendable by two months under specific conditions, with the data subject notified of any extensions within one month. Data controllers under the GDPR must verify requester identity, accept requests via various methods, and exceptions to

[163] Idem.
[164] Miller and Wertheimer, *The Ethics of Consent*. — as per n. 88.

deletion rights include public health and legal claims. Conversely, the Brazilian LGPD requires immediate response or explanation for delays, omitting the need for identity verification. Deletion rights under the LGPD are exercised through express requests, with exceptions for specific processing purposes.[165]

We can see the possibility of using the right to be forgotten, a tool provided by the GDPR, to delete contents from a website or a platform. The procedure is similar to the "notice and takedown", once the individual finds the picture or content, they should notify the data controller (the entity responsible for processing personal data, such as the website owner, photographer, or image hosting platform) about the non-consensual data. Upon receiving a request for the removal of personal data, the data controller or search engine is expected to take appropriate action. This right provides victims with a tool to address non-consensual data listings, placing a significant responsibility on data controllers to assess whether a takedown request based on this right should be accepted. If unsuccessful, the individual may choose to file a complaint with the relevant Data Protection Authority (DPA), the regulatory body responsible for enforcing data protection laws within the jurisdiction of the victim.[166]

Both regulations emphasize consent as pivotal in data processing, aligning with international privacy standards. Consent empowers individuals to control their personal data usage, yet the Brazilian regulation does not fully adopt the reversal of proof burden, instead establishing the joint responsibility of data processors.[167] Despite these characteristics , both regulations hold significance for victims of Non-Consensual Pornography, providing avenues for justice and data control through the right of erasure.

According to the qualitative review performed during the confection of this research, it's understandable that the harms caused by Non-Consensual Pornography are continuous, such as the constant threat and fear regarding the possibility of contents reappearing and disappearing without their control are the main complaints regarding this offense.[168] In order to address these issues, invoking Copyright regulations appear

[165]European Commission. "Data Guidance: GDPR and LGPD." Futurium, https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf.

[166] Aseri, Ankita. 2020. "Juxtaposing Right to Be Forgotten and Copyright Law". *Journal of Intellectual Property Rights* 25 (3&4):100-104. https://ischolar.sscldl.in/index.php/JInctlPR/article/view/203710.

[167] Souza, "Proteção de Dados Pessoais: Estudo Comparado Do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto De Lei Brasileiro N. 5.276/2016"

[168] Henry and Powell, "Sexual Violence in the Digital Age."

here as a quick and effective solution for the victims to remove their content from the internet in a cheaper way, just invoking their rights in situations where private content like images, videos, or conversations are leaked, the copyright holder retains the authority to demand that websites refrain from disseminating or reproducing the material.[169] When the copyright owner possesses rights to an image, seeking cooperation from the uploader is unnecessary as their copyright grants them exclusive control over its distribution and reproduction, enabling them to prevent further dissemination by a website.[170]

If the author of the photo is also its subject or if the victim captured the images themselves, automatic ownership of copyright occurs. The shortcoming is that, conversely, if the photograph is taken by another individual, that person assumes the role of the copyright owner. Similarly, in cases involving digitally manipulated Personal Sexual Imagery (PSI), such as face superimpositions, the copyright belongs to the creator, not the depicted person. However, if an individual was unaware of being recorded or photographed, or had no involvement in the process, as often occurs in videos depicting rape or assault, they lack the ability to utilize copyright protection to control the use of their image in those specific cases.[171]

In cases where victims discover their images or videos on a platform, they can utilize the "notice and takedown" mechanism to mitigate the risk of potential copyright infringement lawsuits. Once a website receives notification that an image is infringing and should be removed, it is obligated to comply. Through this process, a content owner can issue a notification to a website hosting a non-consensual or abusive image (notice), prompting the website to promptly remove it (takedown). While there isn't a specific timeframe for takedown, the Copyright, Designs and Patents Act mandates that service providers must respond swiftly to remove or disable access to the material. This offers victims a quick and cost-effective solution without requiring legal representation.[172]

Finally, this study aimed to cover not just regulatory measures but also practical and technological solutions addressing Non-Consensual Pornography. The discussion

[169] O'Connell and Bakina, "Using IP Rights to Protect Human Rights."
[170] Idem.
[171] Idem.
[172] Aislinn O'Connell and Ksenia Bakina, "Using IP Rights to Protect Human Rights: Copyright for 'Revenge Porn' Removal," *Legal Studies* 40, no. 3 (2020): 442–57, doi:10.1017/lst.2020.17.

surrounding it and its proliferation across social media platforms demands a multifaceted approach that goes beyond regulatory interventions. Understanding user behaviors and leveraging practical and technical remedies are also essential in addressing this pervasive issue, given the urgency of developing effective strategies to combat this offense. With billions of users engaging in social media platforms, the risk of Non-Consensual Pornography dissemination necessitates proactive measures to mitigate harm.[173]

Under this respect some of the most popular Social media platforms, where most of the Non-Consensual Pornography cases happen, saw the need for technological advancements, including machine learning and deep learning algorithms, that offer promising avenues for crime prediction and prevention.

Efforts by companies like Microsoft and Meta to develop tools like PhotoDNA[174] and AI-driven content detection systems represent significant strides in combating Non-Consensual Pornography. These technologies enable the rapid identification and removal of non-consensual intimate content, thereby contributing to safeguard victims and mitigating harm. From those technologies, partnerships between technology companies, law enforcement agencies, and nonprofit organizations were made to further enhance the efficacy of these efforts; for instance platforms like StopNCII.org[175] provide victims with accessible reporting mechanisms and support services, empowering them to take control of their narratives and seek redress.

While social media platforms have implemented enhanced reporting mechanisms and content moderation policies, nevertheless some challenges still persist, as evidenced by the spread of deepfake pornography and the dissemination of explicit content without consent. Addressing the complexities of Non-Consensual Pornography requires a comprehensive approach that combines technological innovation, regulatory frameworks, and community engagement. By leveraging the collective expertise of stakeholders and fostering collaboration, it is possible to create a safer online environment and support victims of non-consensual intimate content. Combating

[173] "Digital 2023 July Global Statshot Report," *DataReportal – Global Digital Insights*, July 20, 2023, https://datareportal.com/reports/digital-2023-july-global-statshot.

[174] "PhotoDNA | Microsoft," accessed February 3, 2024, https://www.microsoft.com/en-us/photodna.

[175] "Resources and Support | StopNCII.Org," accessed January 26, 2024, https://stopncii.org/resources-and-support/.

Non-Consensual Pornography demands continuous vigilance, innovation, and collective action. By harnessing the power of technology responsibly and prioritizing the well-being of users, we can work towards a future where everyone can engage in online spaces free from the threat of exploitation and harm.[176]

However, the extent to which it is possible trusting in the capacity of Artificial Intelligence when it comes to crime prediction shall be critically considered. On one hand, it does not seem reasonable to ignore the existence and the possibilities afforded by machine learning softwares in contrasting Non-Consensual Pornography. However, on the other hand, these technologies cannot be taken into consideration without a closer human evaluation of their limitations and ethical concerns. Biases inherent in the data used to train these algorithms can perpetuate social inequalities and lead to discriminatory outcomes, as those technologies are new and are still being improved.[177]

We can conclude that enhancing the safety of the internet, especially for women and girls, necessitates the refinement of alliances that incorporate mechanisms capable of tracking, locating, and eradicating Non-Consensual Pornography. Furthermore, the development of platforms engineered to deter message dissemination[178], coupled with the integration of human sensibility for data analysis, holds promise as a successful strategy. Such initiatives along with severe and aligned laws against Non-Consensual Pornography, and restorative responses, through understanding victim needs and engaging with affected communities and institutions, swiftly address various harms — includes tackling victim blaming and shaming among peers, family, and teachers, and implementing school-wide strategies against discriminatory bullying [179]— are pivotal in creating not only a secure online environment but also a reality where they feel safe and understood.

---

[176] "Harnessing the Power of AI and Emerging Technologies: Background Paper for the CDEP Ministerial Meeting," OECD Digital Economy Papers, (November 15, 2022), doi:10.1787/f94df8ec-en.

[177] Daniel Maggen, "Law In, Law Out: Legalistic Filter Bubbles and the Algorithmic Prevention of Nonconsensual Pornography," SSRN Scholarly Paper (Rochester, NY, August 31, 2021), https://papers.ssrn.com/abstract=3915143.

[178] Mirko Franco, Ombretta Gaggi, and Claudio E. Palazzi, "Can Messaging Applications Prevent Sexting Abuse? A Technology Analysis," *IEEE Transactions on Mobile Computing*, 2023, 1–14, doi:10.1109/TMC.2023.3238189.

[179] Alexa Dodge, "Restorative Responses to the Rhizomatic Harm of Nonconsensual Pornography," in *The Palgrave Handbook of Gendered Violence and Technology*, ed. Anastasia Powell, Asher Flynn, and Lisa Sugiura (Cham: Springer International Publishing, 2021), 565–82, doi:10.1007/978-3-030-83734-1_28.

References

Alshamsan, Abdullah R, and Shafique A Chaudhry. ‘Detecting Privacy Policies Violations Using Natural Language Inference (NLI)’. In 2022 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 1–6. Gold Coast, Australia: IEEE, 2022. https://doi.org/10.1109/CSDE56538.2022.10089347.

Andrade Guimarães Filho, Pedro, Ariê Scherreier Ferneda, and Miriam Olivia Knopik Ferraz. ‘A Proteção de Dados e a Defesa do Consumidor: Diálogos entre o CDC, o Marco Civil da Internet e a LGPD’. *Revista Meritum* 15 ed 2 (August 2020). https://doi.org/10.46560/meritum.v15i2.7749.

Aseri, Ankita. ‘Juxtaposing Right to Be Forgotten and Copyright Law’. *Journal of Intellectual Property Rights*, 1 July 2020, 100–104. https://ischolar.sscldl.in/index.php/JInctlPR/article/view/203710.

Barrense-Dias, Yara, André Berchtold, Joan-Carles Surís, and Christina Akre. ‘Sexting and the Definition Issue’. *Journal of Adolescent Health* 61, no. 5 (November 2017): 544–54. https://doi.org/10.1016/j.jadohealth.2017.05.009.

Baker, Lisa. Pornhub Receives More Website Traffic Than Amazon and Netflix, New Research Reveals. *Business in the News,* July 19, 2020. Accessed 06 January 2024. URL: https://businessinthenews.co.uk/2020/07/19/pornhub-receives-more-website-traffic-than-amazon-and-netflix-new-research-reveals/.

Bennett, Jessica. ‘The Nudes Aren’t Going Away. Katie Hill’s OK With That.’ *The New York Times*, 8 August 2020, sec. Style. https://www.nytimes.com/2020/08/08/style/katie-hill-she-will-rise-revenge-porn.html.

Benson, Vladlena. *Handbook of Social Media Use Relationships, Security, Privacy, and Society.* Volume 2. [S.l.]: Academic Press, 2023.

Bhattacharya, J., R. Dass, V. Kapoor, and S.K. Gupta. ‘Utilizing Network Features for Privacy Violation Detection’. In 2006 *1st International Conference on Communication Systems Software & Middleware*, 1–10. New Delhi, India: IEEE, 2006. https://doi.org/10.1109/COMSWA.2006.1665184.

Breen, Stephen, Karim Ouazzane, and Preeti Patel. ‘GDPR: Is Your Consent Valid?’ *Business Information Review* 37, no. 1 (March 2020): 19–24. https://doi.org/10.1177/0266382120903254.

Carvalho, Ana C., Rolando Martins, and Luis Antunes. ‘How-to Express Explicit and Auditable Consent’. In 2018 *16th Annual Conference on Privacy, Security and Trust (PST)*, 1–5. Belfast: IEEE, 2018. https://doi.org/10.1109/PST.2018.8514204.

Carvalho, Julio. *A Cultural History of Copyright: From Books to Networks.* Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-46854-4.

Comella, Lynn, and Shira Tarrant, eds. *New Views on Pornography: Sexuality, Politics, and the Law.* Santa Barbara, California: Praeger, an imprint of ABC-CLIO, LLC, 2015.

Conroy, Amy A., Allison Ruark, and Judy Y. Tan. ‘Re-Conceptualising Gender and Power Relations for Sexual and Reproductive Health: Contrasting Narratives of Tradition, Unity, and Rights’. *Culture, Health & Sexuality* 22, no. sup1 (20 April 2020): 48–64. https://doi.org/10.1080/13691058.2019.1666428.

Conselho Nacional do Ministério Público. *Fundamentos e Princípios.* Accessed 12 February 2024. https://www.cnmp.mp.br/portal/transparencia/lei-geral-de-protecao-de-dados-pessoais-lgpd/a-lgpd/fundamentos-e-principios.

Cyber Rights Organization. ‘Cyber Rights Organization’. Accessed 12 February 2024. https://cyberights.org/.

Data Protection Commission. ‘Principles of Data Protection’. Accessed 12 February 2024. https://www.dataprotection.ie/individuals/data-protection-basics/principles-data-protection.

Data Reportal – Global Digital Insights. ‘Digital 2023 July Global Statshot Report’, 20 July 2023. https://datareportal.com/reports/digital-2023-july-global-statshot.

Dodge, Alexa. ‘Nudes Are Forever: Judicial Interpretations of Digital Technology’s Impact on “Revenge Porn”’. *Canadian Journal of Law and Society / La Revue*

Canadienne Droit et Société 34, no. 1 (April 2019): 121–43. https://doi.org/10.1017/cls.2019.4.

Dodge, Alexa. Restorative Responses to the Rhizomatic Harm of Nonconsensual Pornography. In *The Palgrave Handbook of Gendered Violence and Technology,* edited by Anastasia Powell, Asher Flynn, and Lisa Sugiura, 565–82. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-83734-1_28.

Duarte, Larissa Costa, and Fabiola Rohden. 'Entre o Obsceno e o Científico: Pornografia, Sexologia e a Materialidade Do Sexo'. *Revista Estudos Feministas* 24, no. 3 (December 2016): 715–37. https://doi.org/10.1590/1806-9584-2016v24n3p715.

Döring, Nicola, and M. Rohangis Mohseni. 'Are Online Sexual Activities and Sexting Good for Adults' Sexual Well-Being? Results From a National Online Survey'. *International Journal of Sexual Health* 30, no. 3 (3 July 2018): 250–63. https://doi.org/10.1080/19317611.2018.1491921.

Eurojust | Copyright Infringement Notice | European Union Agency for Criminal Justice Cooperation. Accessed 12 February 2024. https://www.eurojust.europa.eu/publication/copyright-infringement-notice.

European Commission. "Data Guidance: GDPR and LGPD." Futurium, https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf. Accessed January 13, 2024.

European Parliament Research Service. "Violence against women in the EU." European Parliament. 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739208/EPRS_BRI%282022%29739208_EN.pdf

European Union Agency for Fundamental Rights. 'Violence against Women: An EU-Wide Survey. Main Results Report', 3 February 2014. http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report.

Facebook Help Center. Report Content on Facebook. Accessed January 30, 2024. https://www.facebook.com/help/1380418588640631

Facebook Help Center. Reporting Conversations. Accessed January 30, 2024. https://www.facebook.com/help/messenger-app/1165699260192280/

Facebook. "Sexual Exploitation of Adults." Facebook Community Standards. Accessed January 21, 2024. https://transparency.fb.com/en-gb/policies/community-standards/sexual-exploitation-adults/?source=https%3A%2F%2Fwww.facebook.com%2Fcommunitystandards%2Fsexual_exploitation_adults

Facebook: Send Us Your Naked Photos to Stop Revenge Porn - CBS News', 24 May 2018. https://www.cbsnews.com/news/facebook-revenge-porn-naked-photos-pilot-progam/.

Falduti, Mattia, and Sergio Tessaris. 'Mapping the Interdisciplinary Research on Non-Consensual Pornography: Technical and Quantitative Perspectives'. *Digital Threats: Research and Practice* 4, no. 3 (30 September 2023): 1–22. https://doi.org/10.1145/3608483.

Fórum Brasileiro de Segurança Pública. *Visível e Invisível: A Vitimização de Mulheres no Brasil*. 4. ed. São Paulo: FBSP, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/03/visiveleinvisivel-2023-relatorio.pdf. Acesso em: 2 fev. 2024.

Finkelstein, Maria Eugenia, and Claudio Finkelstein. 'Privacidade e Lei Geral de Proteção de Dados Pessoais'. *Revista de Direito Brasileira* 23, no. 9 (11 February 2020): 284. https://doi.org/10.26668/IndexLawJournals/2358-1352/2019.v23i9.5343.

Franco, Mirko, Ombretta Gaggi, and Claudio E. Palazzi. 'Can Messaging Applications Prevent Sexting Abuse? A Technology Analysis'. *IEEE Transactions on Mobile Computing,* 2023, 1–14. https://doi.org/10.1109/TMC.2023.3238189.

Frankel, Anne S., Sarah Bauerle Bass, Freda Patterson, Ting Dai, and Deanna Brown. 'Sexting, Risk Behavior, and Mental Health in Adolescents: An Examination of 2015 Pennsylvania Youth Risk Behavior Survey Data'. *Journal of School Health* 88, no. 3 (March 2018): 190–99. https://doi.org/10.1111/josh.12596.

Garcez, Gabriela Soldano, and Izabela Clementino De Miranda Gonçalves. ‘Obstáculos Na Proteção Do Direito à Privacidade e Da Honra Da Mulher Na Internet’. *LEOPOLDIANUM* 49, no. 138 (1 September 2023): 16. https://doi.org/10.58422/releo2023.e1419.

Ghorashi, Seyed Ramin, Tanveer Zia, Michael Bewong, and Yinhao Jiang. ‘An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing’. *Applied Sciences* 13, no. 23 (27 November 2023): 12727. https://doi.org/10.3390/app132312727.

Graham Holmes, Laura, A. Renee Nilssen, Deanna Cann, and Donald S. Strassberg. ‘A Sex-Positive Mixed Methods Approach to Sexting Experiences among College Students’. *Computers in Human Behavior.* Volume 115 (February 2021): 106619. https://doi.org/10.1016/j.chb.2020.106619.

Grimaldi, Cecilia. ‘A Post for Change: Social Media and the Unethical Dissemination of Nonconsensual Pornography’. *UC Law SF Communications and Entertainment Journal* 43, no. 1 (1 January 2021): 109. https://repository.uclawsf.edu/hastings_comm_ent_law_journal/vol43/iss1/5.

Gámez-Guadix, Manuel, and Estibaliz Mateos-Pérez. ‘Longitudinal and Reciprocal Relationships between Sexting, Online Sexual Solicitations, and Cyberbullying among Minors’. *Computers in Human Behavior.* Volume 94 (May 2019): 70–76. https://doi.org/10.1016/j.chb.2019.01.004.

Gámez-Guadix, Manuel, Carmen Almendros, Erika Borrajo, and Esther Calvete. ‘Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults’. *Sexuality Research and Social Policy* 12, no. 2 (June 2015): 145–54. https://doi.org/10.1007/s13178-015-0186-9.

Gámez‐Guadix, Manuel, Estibaliz Mateos‐Pérez, Sebastian Wachs, Michelle Wright, Jone Martínez, and Daniel Íncera. ‘Assessing Image‐based Sexual Abuse: Measurement, Prevalence, and Temporal Stability of Sextortion and Nonconsensual Sexting (“Revenge Porn”) among Adolescents’. *Journal of Adolescence* 94, no. 5 (July 2022): 789–99. https://doi.org/10.1002/jad.12064.

Goujard, Clothilde. ‘EU Countries Reject Making Non-Consensual Sex a Criminal Offense across the Bloc’, 9 June 2023. https://www.politico.eu/article/rape-europe-criminal-offense-non-consensual-sex/.

Hampton, Jean. ‘Punishment, Feminism, and Political Identity: A Case Study in the Expressive Meaning of the Law’. *Canadian Journal of Law & Jurisprudence* 11, no. 1 (January 1998): 23–45. https://doi.org/10.1017/S0841820900001673.

Harnessing the Power of AI and Emerging Technologies: Background Paper for the CDEP Ministerial Meeting’. *OECD Digital Economy Papers*, 15 November 2022. https://doi.org/10.1787/f94df8ec-en.

Henry Nicola, Flynn Asher, and Powell Anastasia. *Responding to 'Revenge Pornography': Prevalence, Nature and Impacts.* Criminology Research Grants Program, Australian Institute of Criminology, 2019.

Henry, Nicola, and Anastasia Powell. ‘Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law’. *Social & Legal Studies* 25, no. 4 (August 2016): 397–418. https://doi.org/10.1177/0964663915624273.

Hill, Kashmir. ‘Why We Find Hunter Moore And His “Identity Porn” Site, IsAnyoneUp, So Fascinating’. *Forbes.* Accessed 12 February 2024. https://www.forbes.com/sites/kashmirhill/2012/04/05/hunter-moore-of-isanyoneup-wouldnt-mind-making-some-money-off-of-a-suicide/.

Home Security Heroes. 2023 State Of Deepfakes: Realities, Threats, And Impact. Accessed 12 February 2024. https://www.homesecurityheroes.com/state-of-deepfakes/.

Instagram Help Center. Privacy and Safety Center. Accessed January 30, 2024. https://help.instagram.com/165828726894770?ref=ig_about

Intellectual Property Rights Office | Copyright History. Accessed 12 February 2024. https://intellectualpropertyrightsoffice.org/copyright_history/?v=99ED03F0-D0D6-4406-B94E-548067279E5.

Jaiswal, Hrishikesh. ‘Memes, Confession Pages and Revenge Porn- The Novel Forms of Cyberbullying’. *SSRN Electronic Journal,* 2021. https://doi.org/10.2139/ssrn.3816609.

Jones, Simon. ‘Revenge Porn Victims Suffering in Silence - Survey Shows Law Not Fit for Purpose and Needs to Change’. *Police, Fire and Crime Commissioner North Yorkshire,* 20 November 2018. https://www.northyorkshire-pfcc.gov.uk/news/revenge-porn-victims-suffering-in-silence-survey-shows-law-not-fit-for-purpose-and-needs-to-change/.

Ke, T. Tony, and K. Sudhir. ‘Privacy Rights and Data Security: GDPR and Personal Data Markets’. *Management Science* 69, no. 8 (August 2023): 4389–4412. https://doi.org/10.1287/mnsc.2022.4614.

Kelly, Caitlin. ‘Facebook’s Anti-Revenge Porn Tools Failed to Protect Katie Hill’. *Wired.* Accessed 12 February 2024. https://www.wired.com/story/katie-hill-revenge-porn-facebook/.

Kristof, Nicholas. ‘Opinion | The Children of Pornhub’. *The New York Times*, 4 December 2020, sec. Opinion. https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html.

Kshatri, Sapna Singh, Deepak Singh, Bhavana Narain, Surbhi Bhatia, Mohammad Tabrez Quasim, and G. R. Sinha. ‘An Empirical Analysis of Machine Learning Algorithms for Crime Prediction Using Stacked Generalization: An Ensemble Approach’. *IEEE Access* 9 (2021): 67488–500. https://doi.org/10.1109/ACCESS.2021.3075140.

Lenhart, Amanda, Michele Ybarra, Kathryn Zickuhr, and Myeshia Price-Feeney. ‘Online Harassment, Digital Abuse, and Cyberstalking in America’. *Data & Society,* 21 November 2016. https://datasociety.net/library/online-harassment-digital-abuse-cyberstalking/.

Levendowski, Amanda. ‘Using Copyright to Combat Revenge Porn’. *NYU Journal of Intellectual Property & Entertainment Law* (blog), 1 May 2014. https://jipel.law.nyu.edu/vol-3-no-2-6-levendowski/.

Lindroos-Hovinheimo, Susanna. ‘Jurisdiction and Personality Rights – in Which Member State Should Harmful Online Content Be Assessed?’ *Maastricht Journal of European and Comparative Law* 29, no. 2 (April 2022): 201–14. https://doi.org/10.1177/1023263X221076392.

Loh, Kep Kee, and Ryota Kanai. ‘How Has the Internet Reshaped Human Cognition?’ *The Neuroscientist* 22, no. 5 (October 2016): 506–20. https://doi.org/10.1177/1073858415595005.

Madigan, Sheri, Anh Ly, Christina L. Rash, Joris Van Ouytsel, and Jeff R. Temple. ‘Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-Analysis’. *JAMA Pediatrics* 172, no. 4 (1 April 2018): 327. https://doi.org/10.1001/jamapediatrics.2017.5314.

Mandalapu, Varun, Lavanya Elluri, Piyush Vyas, and Nirmalya Roy. ‘Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions’. *IEEE Access* 11 (2023): 60153–70. https://doi.org/10.1109/ACCESS.2023.3286344.

McGlynn, Clare, Erika Rackley, and Ruth Houghton. ‘Beyond “Revenge Porn”: The Continuum of Image-Based Sexual Abuse’. *Feminist Legal Studies* 25, no. 1 (April 2017): 25–46. https://doi.org/10.1007/s10691-017-9343-2.

McGlynn, Clare, Kelly Johnson, Erika Rackley, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. ‘“It’s Torture for the Soul”: The Harms of Image-Based Sexual Abuse’. *Social & Legal Studies* 30, no. 4 (August 2021): 541–62. https://doi.org/10.1177/0964663920947791.

Meta. "Bullying & Harassment." Meta, Accessed January 2022. https://about.meta.com/actions/safety/topics/bullying-harassment/ncii/pilot.

Meta. ‘Strengthening Our Efforts Against the Spread of Non-Consensual Intimate Images’, 2 December 2021. https://about.fb.com/news/2021/12/strengthening-efforts-against-spread-of-non-consensual-intimate-images/.

Meta. The Facts: Non-Consensual Intimate Image Pilot. 9 November 2017, accessed 21 January 2024
https://about.fb.com/news/h/non-consensual-intimate-image-pilot-the-facts/.,‘PhotoDNA FAQ | Microsoft’, accessed 21 January 2024
https://www.microsoft.com/en-us/photodna/faq.

Microsoft. PhotoDNA Cloud Service. Accessed 12 February 2024.
https://www.microsoft.com/en-us/photodna/cloudservice.

Miller, Franklin G., and Alan Wertheimer, eds. *The Ethics of Consent: Theory and Practice*. Oxford ; New York: Oxford University Press, 2010.

Molla-Esparza, Cristian, Emelina López-González, and Josep-María Losilla. ‘Sexting Prevalence and Socio-Demographic Correlates in Spanish Secondary School Students’. *Sexuality Research and Social Policy* 18, no. 1 (March 2021): 97–111. https://doi.org/10.1007/s13178-020-00434-0.

Mondschein, Christopher F., and Cosimo Monda. ‘The EU’s General Data Protection Regulation (GDPR) in a Research Context’. In *Fundamentals of Clinical Data Science*, edited by Pieter Kubben, Michel Dumontier, and Andre Dekker, 55–71. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-319-99713-1_5.

Morelli, Mara, Dora Bianchi, Roberto Baiocco, Lina Pezzuti, and Antonio Chirumbolo. ‘Sexting, Psychological Distress and Dating Violence among Adolescents and Young Adults’. *Psicothema*, 2016.
https://redined.educacion.gob.es/xmlui/handle/11162/118365.

Nascimento Maia, Mariana, and Rafael Baioni Do Nascimento. ‘Pornografia de Vingança No Ordenamento Jurídico-Penal Brasileiro’. *Confluências. Revista Interdisciplinar de Sociologia e Direito* 24, no. 2 (1 August 2022): 104–25. https://doi.org/10.22409/conflu.v24i2.53554.

Nguyen, Tna. ‘European “Right To Be Forgotten” as a Remedy For Image-Based Sexual Abuse: a Critical Review’. *KnowEx Social Sciences*, 25 July 2022, 59–72. https://doi.org/10.17501/27059901.2021.2105.

Oliveira, Caroline Lujan De, Antonieta Ferreira Machado De Oliveira, and Carolina Yukari Veludo Watanabe. ‘Utilização de Dados Pessoais Pelas Empresas: LGPD e o Comportamento Do Consumidor Com o Macro Modelo APCO / Use of Personal Data by Companies: LGPD and Consumer Behavior with the Macro Model APCO’. *Brazilian Journal of Development* 7, no. 6 (28 June 2021): 63580–91. https://doi.org/10.34117/bjdv7n6-641.

O’Neil Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, First Edition (New York: Crown, 2016).

Patchin, Justin W., and Sameer Hinduja. ‘Sextortion Among Adolescents: Results From a National Survey of U.S. Youth’. *Sexual Abuse* 32, no. 1 (February 2020): 30–54. https://doi.org/10.1177/1079063218800469.

Patella-Rey, Pj. ‘Beyond Privacy: Bodily Integrity as an Alternative Framework for Understanding Non-Consensual Pornography’. *Information, Communication & Society* 21, no. 5 (4 May 2018): 786–91. https://doi.org/10.1080/1369118X.2018.1428653.

Patrick, Kent, Wendy Heywood, Marian K. Pitts, and Anne Mitchell. ‘Demographic and Behavioural Correlates of Six Sexting Behaviours among Australian Secondary School Students’. *Sexual Health* 12, no. 6 (2015): 480. https://doi.org/10.1071/SH15004.

Peters, Tobias M., and Roel W. Visser. ‘The Importance of Distrust in AI’. In Explainable Artificial Intelligence, edited by Luca Longo, 301–17. *Communications in Computer and Information Science.* Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-44070-0_15.

Pienta, Amy, Joy Jang, and Margaret Levenstein. ‘Beyond Legal Frameworks and Security Controls For Accessing Confidential Survey Data: Engaging Data Users in Data Protection’. *Journal of Privacy and Confidentiality* 13, no. 2 (6 December 2023). https://doi.org/10.29012/jpc.845.

Powell, Anastasia, Nicola Henry, Asher Flynn, and Adrian J. Scott. ‘Image-Based Sexual Abuse: The Extent, Nature, and Predictors of Perpetration in a Community Sample of Australian Residents’. *Computers in Human Behavior* 92 (March 2019): 393–402. https://doi.org/10.1016/j.chb.2018.11.009.

Rackley, Erika, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn, and Anastasia Powell. ‘Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse’. *Feminist Legal Studies* 29, no. 3 (November 2021): 293–322. https://doi.org/10.1007/s10691-021-09460-8.

Rádio Senado. ‘Dez anos de vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos’. Accessed 12 February 2024. https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos.

Rafi, Amir, Carlton Shepherd, and Konstantinos Markantonakis. ‘A First Look at Digital Rights Management Systems for Secure Mobile Content Delivery’, 2023. https://doi.org/10.48550/ARXIV.2308.00437.

Ruvalcaba, Yanet, and Asia A. Eaton. ‘Nonconsensual Pornography among U.S. Adults: A Sexual Scripts Framework on Victimization, Perpetration, and Health Correlates for Women and Men.’ *Psychology of Violence* 10, no. 1 (January 2020): 68–78. https://doi.org/10.1037/vio0000233.

SaferNet Brasil | accessed February 10, 2024, https://new.safernet.org.br/.

Safety and Security Online | SWGfL accessed February 10, 2024, https://swgfl.org.uk/.

Santos, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais (Lei n. 13.709/2018), 25 September 2019. http://repositorio.uniceub.br/jspui/handle/prefix/13802.

Scarpatto, Carolina, Giovana Ilka Jacinto Salvaro, and Mônica Ovinski De Camargo. ‘Women in Situations of Violation of Privacy: Psychological and Moral Damage in the Context of Gender Violence’. *Aletheia* 56, no. 1 (2023): 71–92. https://doi.org/10.4322/aletheia.005.en.

Shah, Neil, Nandish Bhagat, and Manan Shah. ‘Crime Forecasting: A Machine Learning and Computer Vision Approach to Crime Prediction and Prevention’. *Visual Computing for Industry, Biomedicine, and Art 4*, no. 1 (29 April 2021): 9. https://doi.org/10.1186/s42492-021-00075-z.

Souza, Luíza Ribeiro De Menezes. ‘Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016.’ *Caderno Virtual* 1, no. 41 (2 March 2018). https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153.

StopNCII.Org. Resources and Support. Accessed 12 February 2024. https://stopncii.org/resources-and-support/.

Strohmaier, Heidi, Megan Murphy, and David DeMatteo. ‘Youth Sexting: Prevalence Rates, Driving Motivations, and the Deterrent Effect of Legal Consequences’. *Sexuality Research and Social Policy* 11, no. 3 (September 2014): 245–55. https://doi.org/10.1007/s13178-014-0162-9.

Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma, Violence, & Abuse* 19, no. 2 (April 2018): 195–208. https://doi.org/10.1177/1524838016650189.

Telegram. ‘Telegram Privacy Policy’. Accessed 12 February 2024. https://telegram.org/privacy.

Tepedino, Gustavo, Ana Frazão, and Milena Donato Oliva. ‘Lei geral de proteção de dados pessoais: e suas repercussões no direito brasileiro’, 2023. https://bdjur.stj.jus.br/jspui/handle/2011/139297.

Tepedino, Gustavo, and Chiara Spadaccini De Teffé. ‘O Consentimento na Circulação de Dados Pessoais’. *Revista Brasileira de Direito Civil* 25, no. 03 (2020). https://doi.org/10.33242/rbdc.2020.03.005.

Tsohou, Aggeliki, and Thanos Papaioannou. ‘Impacts of Information Privacy Violations’. *In Encyclopedia of Cryptography, Security and Privacy*, edited by Sushil Jajodia, Pierangela Samarati, and Moti Yung, 1–4. Berlin, Heidelberg: Springer, 2019. https://doi.org/10.1007/978-3-642-27739-9_1614-1.

Umeike, Robinson. ‘Comparative Crime Analysis and Prediction Using Machine Learning Algorithms: Assessing the Tools and Addressing the Threats’. In *2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI)*, 135–42. Atlanta, GA, USA: IEEE, 2023. https://doi.org/10.1109/ICTAI59109.2023.00027.

United Nations Population Fund. ‘Bodyright - Own Your Body Online | Bodily Integrity | UNFPA’. Accessed 12 February 2024. https://www.unfpa.org/bodyright/.

Van Ouytsel, Joris, Michel Walrave, and Koen Ponnet. ‘An Exploratory Study of Sexting Behaviors Among Heterosexual and Sexual Minority Early Adolescents’. *Journal of Adolescent Health* 65, no. 5 (November 2019): 621–26. https://doi.org/10.1016/j.jadohealth.2019.06.003.

Veena, K., K. Meena, Ramya Kuppusamy, Yuvaraja Teekaraman, Ravi V. Angadi, and Amruth Ramesh Thelkar. ‘Cybercrime: Identification and Prediction Using Machine Learning Techniques’. Edited by Dalin Zhang. *Computational Intelligence and Neuroscience* 2022 (27 August 2022): 1–10. https://doi.org/10.1155/2022/8237421.

Voigt, Paul, and Axel Von Dem Bussche. *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-57959-7.

Wachs, Sebastian, Michelle F. Wright, Manuel Gámez-Guadix, and Nicola Döring. ‘How Are Consensual, Non-Consensual, and Pressured Sexting Linked to Depression and Self-Harm? The Moderating Effects of Demographic Variables’. *International Journal of Environmental Research and Public Health* 18, no. 5 (5 March 2021): 2597. https://doi.org/10.3390/ijerph18052597.

Walker, Kate, and Emma Sleath. ‘A Systematic Review of the Current Knowledge Regarding Revenge Pornography and Non-Consensual Sharing of Sexually Explicit Media’. *Aggression and Violent Behavior* 36 (September 2017): 9–24. https://doi.org/10.1016/j.avb.2017.06.010.

Ward, Zara. "Revenge Porn Helpline Annual Report 2022." Accessed 30 January 2024. URL: https://revengepornhelpline.org.uk/assets/documents/rph-report-2022.pdf.

Wolak, Janis, David Finkelhor, Wendy Walsh, and Leah Treitman. ‘Sextortion of Minors: Characteristics and Dynamics’. *Journal of Adolescent Health* 62, no. 1 (January 2018): 72–79. https://doi.org/10.1016/j.jadohealth.2017.08.014.

X Help. X’s Non-Consensual Nudity Policy. Accessed 12 February 2024. https://help.twitter.com/en/rules-and-policies/intimate-media.

Yoon, Cynthia, Rebecca L. Emery, Susan M. Mason, and Dianne Neumark-Sztainer. ‘Sexual and Physical Abuse and Identity of the Perpetrator: Associations with Binge Eating and Overeating in Project EAT 2018’. *Eating Behaviors* 43 (December 2021): 101577. https://doi.org/10.1016/j.eatbeh.2021.101577.

Završnik, Aleš. ‘Algorithmic Justice: Algorithms and Big Data in Criminal Justice Settings’. *European Journal of Criminology* 18, no. 5 (September 2021): 623–42. https://doi.org/10.1177/1477370819876762.

Zlotnick, Caron, Ann Begin, M.Tracie Shea, Teri Pearlstein, Elizabeth Simpson, and Ellen Costello. ‘The Relationship between Characteristics of Sexual Abuse and Dissociative Experiences’. *Comprehensive Psychiatry* 35, no. 6 (November 1994): 465–70. https://doi.org/10.1016/0010-440X(94)90230-5.

Zylberkan, Mariana. ‘Sexo e internet: quando a exposição pode levar à morte’. Accessed 12 February 2024. https://veja.abril.com.br/brasil/sexo-e-internet-quando-a-exposicao-pode-levar-a-morte/.

Legislative Acts

Brasil. Código Civil de 2002. Available at: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm

Brasil. Constituição da República Federativa do Brasil de 1988. Available at: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

Brasil. Decreto-Lei No. 2.848 de 7 de Dezembro de 1940. Código Penal. Available at: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

Brasil. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Available at: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Brasil. Lei Geral de Proteção de Dados Pessoais. Lei nº 13.709, de 14 de agosto de 2018. Available at: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm.

Brasil. Constituição (1988) Emendas, ‘Constitution of the Federative Republic of Brazil: Constitutional Text of October 5, 1988, with the Alterations Introduced by Constitutional Amendments No. 1/92 through 72/2013 and by Revision Constitutional Amendments No. 1/94 through 6/94’, 2013, accessed 24 January 2024 https://www2.senado.gov.br/bdsf/handle/id/243334.

Brasil.“General Data Protection Law (LGPD, English Translation),” accessed February 10, 2024, https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

European Union. “Directive - 2000/31 - EN - e-Commerce Directive - EUR-Lex,” accessed January 25, 2024, https://eur-lex.europa.eu/eli/dir/2000/31/oj.

European Union. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data." Official Journal of the European Communities, L 281, 23 November 1995. Accessed January 25, 2024. http://data.europa.eu/eli/dir/1995/46/oj.

European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data." Official Journal of the European Union, L 119, 4 May 2016. Accessed January 25, 2024. http://data.europa.eu/eli/reg/2016/679/oj.

Spain. ‘Ley 27/2003, de 31 de Julio, Reguladora de La Orden de Protección de Las Víctimas de La Violencia Doméstica’, Pub. L. No. Ley 27/2003, § 1, 29881 (2003), accessed 25 January 2024 https://www.boe.es/eli/es/l/2003/07/31/27.

UK Legislation. “Abusive Behaviour and Sexual Harm (Scotland) Act 2016,” accessed February 10, 2024, https://www.legislation.gov.uk/asp/2016/22/section/2/enacted?view=plain.

UK Legislation. "Children and Young People (Scotland) Act 2016, Section 2." Accessed January 25, 2024. https://www.legislation.gov.uk/asp/2016/22/section/2/enacted?view=plain.

UK Legislation. “Criminal Justice and Courts Act 2015,” accessed February 10, 2024, https://www.legislation.gov.uk/ukpga/2015/2/section/33/enacted?view=plain.

UK Legislation. "Copyright, Designs and Patents Act 1988, Part I, Chapter I, Crossheading: Authorship and Ownership of Copyright." Accessed January 25, 2024. https://www.legislation.gov.uk/ukpga/1988/48/part/I/chapter/I/crossheading/authorship-and-ownership-of-copyright.

UK Legislation. "Data Protection Act 1988, Section 1." Accessed January 25, 2024. https://www.legislation.gov.uk/ukpga/1988/48/section/1?view=plain.

UK Legislation. "The Treaty of Union 1707." Accessed January 25, 2024. https://www.legislation.gov.uk/aep/Ann/6/8.

UK Legislation. "Welfare Reform (Northern Ireland) Act 2016, Section 51." Accessed January 25, 2024. https://www.legislation.gov.uk/nia/2016/21/section/51/enacted?view=plain.

United Nations. "Universal Declaration of Human Rights (1948)." Accessed January 25, 2024. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

United States of America “U.S.C. Title 17 - COPYRIGHTS,” accessed February 10, 2024, https://www.govinfo.gov/content/pkg/USCODE-2022-title17/html/USCODE-2022-title17-chap5-sec512.htm.

World Intellectual Property Organization. "Spanish Patent Act (Revised Text)." Accessed January 25, 2024. https://wipolex-res.wipo.int/edocs/lexdocs/laws/en/es/es020en.pdf.