

# **Exploring digital sexual crimes, accountability, and adjudication in The Netherlands: the intersection of research, education and collaborative online learning**

Thesis student: Aisha Aziz (Law)

Thesis supervisor: Ms. Linda Louis (Law)

MLR contact person: Dr. Anna Matczak (SSMS)

## **Introduction**

This thesis aims to assess the adequacy of Dutch law in addressing technology-facilitated sexual violence (hereinafter TFSV), explore the challenges in enforcing the laws, and provide recommendations for improving their implementation. The thesis is based on a legal analysis of digital sexual crimes, accountability, and adjudication in the Netherlands, with a focus on the effects on women and girls. It includes interviews with three professionals in the field: a psychology expert at the Centre for Sexual Violence, an expert from the Netherlands Institute for the Study of Crime and Law Enforcement, and an academic specialising in relevant studies.

## **Connection to the Multilevel Regulation framework**

Multi-level regulation (hereinafter MLR) refers to a governance approach where regulatory responsibilities are dispersed among various actors, including international, supranational, or national entities. In practice, these levels often overlap and are not isolated, allowing for a comprehensive understanding of all the actors involved in resolving an issue and how their tasks intertwine. The MLR Research Group focuses on addressing legal challenges by working with private actors on different levels to ensure constant adaptation of public regulation, as well as on exploring topics that aim to challenge traditional regulation of the law. As technology is an ever-evolving field so are its impacts on society, thus the research group would like to explore ways in which the effects can be reduced.

The MLR framework is crucial to fully grasp the complexity and multi-agency approach of legal responses to harms, such as the accelerating TFSV. This significance stems from MLR's ability to navigate the intricate networks, diverse actors, and varied practices that govern TFSV offenses.<sup>1</sup> The significance of MLR becomes evident in understanding the intricate complexities of TFSV. As TFSV often lies in being a borderless crime, outside the traditional framework of a face-to-face crime, combating it requires a broader perspective that requires multiple jurisdictions and multiple facets to combat. In its nature, MLR is able to integrate different actors and norms from different levels, including international organizations, private corporations, NGOs, and other bodies beyond the state actor. Therefore, the incorporation of MLR in combating the multi-faceted issue of TFSV is essential as it may span over multiple jurisdictions and different levels of actors and affects in some cases victims in more than one jurisdiction.

Additionally, in 2023, the MLR lecturer-researcher, Dr. Anna Matczak, successfully obtained a VIS grant (Virtuele Internationale Samenwerking), an initiative funded by the Dutch Ministry of Education, Culture, and Science to foster online collaborations between students from different countries. In this case, the project entailed a collaboration between the [Safety and Security Management Studies programme](#) at THUAS, and its counterpart, [the Public Safety and Security programme](#), at the

---

<sup>1</sup>B Warwas, 'Returning to the Origins of Multilevel Regulation: The Role of Historical ADR Practices' (15 July 2021).

University of Social Sciences in Singapore. Working together, students from both institutions conducted research on the impact of technology-facilitated sexual violence on the respective university students. Further, the project provided me with an opportunity to work as a project tutor, guiding the group of students throughout my own thesis writing process. I will reflect on this experience at the end of the summary.

### What is TFSV?

Scholars typically define technology in relation to TFSV in three ways. The first broadly considers technology as technical artifacts, implying it is merely a 'tool' used to facilitate harm. The second refers to technology as something that amplifies or extends human capability, while the third views technology as an entity that invites or promotes the commission of violence.<sup>2</sup>

While TFSV has not been given a uniform definition, it is often understood as unwanted or unwelcome sexual behaviour involving the use of technology. This includes online harassment, image-based abuse (such as revenge porn), and online sexual aggression/coercion.<sup>3</sup> It also encompasses the distribution of sexual images and messages without prior consent (sextortion).<sup>4</sup> For this report, TFSV will be referenced as a spectrum of behaviours where digital technologies are used to facilitate virtual sexual-based harms<sup>5</sup>, which can be manifested in the following forms:

<i>Type of TFSV</i>	<i>Definition</i>
<u><i>Revenge Porn</i></u>	A form of image-based abuse; a preferred term is non-consensual sharing of intimate imagery. While commonly used, “revenge porn” is objectionable as it suggests consent from and wrongdoing by the survivor to provoke retribution. <sup>6</sup>
<u><i>Online Harassment</i></u>	Repeated conduct that threatens, pesters, scares, or abuses someone by sending degrading, offensive, or insulting comments or images. <sup>7</sup>

<sup>2</sup> Mitchell M, Wood J, O'Neill T, Wood M, Pervan F, Anderson B and Arpke-Wales W, 'Technology-Facilitated Violence: A Conceptual Review' (2022) *Criminology & Criminal Justice*, <https://doi.org/10.1177/17488958221140549>, 5.

<sup>3</sup> Champion A, Oswald F, Khera D and Pedersen C, 'Examining the Gendered Impacts of Technology-Facilitated Sexual Violence: A Mixed Methods Approach' (2022) 51 *Archives of Sexual Behavior*.

<sup>4</sup> Naezer M and van Oosterhout L, 'Only Sluts Love Sexting: Youth, Sexual Norms and Non-Consensual Sharing of Digital Sexual Images' (2021) 30(1) *Journal of Gender Studies* 79-90.

<sup>5</sup> Henry N and Powell A, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 19(2) *Trauma, Violence, & Abuse* 195-208.

<sup>6</sup> Henry N, Gavey N and Johnson K, 'Image-Based Sexual Abuse as a Means of Coercive Control: Victim-Survivor Experiences' (2023) 29(6-7) *Violence Against Women* 1123 <https://doi.org/10.1177/10778012221114918>.

<sup>7</sup> Wolak J, Mitchell KJ and Finkelhor D, 'Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts' (2007) 41(6) *Journal of Adolescent Health* 551-558.

Sextortion

A type of electronic extortion, the demand for money, sex/sex acts, or additional explicit images in exchange for not exposing intimate images or private information.<sup>8</sup>

Image-Based Abuse

The use of imagery, often sexual, to objectify, exploit, humiliate, or harass. Examples include non-consensual sharing of intimate imagery aka non-consensual porn and child sexual abuse material (showing minors in sexually explicit situations).<sup>9</sup>

Deep fake images

A manipulated image is often done with editing software, such as attaching someone's face to someone else's body. A more believable, sophisticated deepfake is done with machine learning.

## **International legal TFSV landscape**

The legal analysis was carried out in this thesis on three levels: international, European, and national. Although no comprehensive international legal framework specifically addresses TFSV is available, various articles and treaties can be combined to understand the international stance on this issue. Notably, the Convention on the Elimination of All Forms of Discrimination Against Women (hereinafter CEDAW) obliges states to amend legislation to eradicate gender-based discrimination. General Recommendation No. 35 expands on this, recognizing the prohibition of gender-based violence as a norm of international customary law and broadening the definition of violence to include sexual violence. It also emphasizes the need for different levels of state liability for acts related to violence and calls for the repeal of laws and policies that indirectly excuse, condone, and facilitate violence.<sup>10</sup>

Although General Recommendation No. 35 and CEDAW do not specifically address online sexual violence, their broad framework and principles can be applied to all forms of gendered violence, including those facilitated through technology.<sup>11</sup> Similarly, the Convention on the Rights of the Child (CRC) focuses on the protection of children, addressing the criminalization of sexual exploitation against children. Furthermore, the Budapest Convention, specifically Article 9, mandates states to criminalize child pornography, including material accessed via computers.

While none of the above frameworks directly address online sexual violence, their principles can be applied to all forms of gender violence, including those facilitated by technology. However, the

---

<sup>8</sup>Wolak J, Mitchell KJ and Finkelhor D, 'Does Online Harassment Constitute Bullying? An Exploration of Online Harassment by Known Peers and Online-Only Contacts' (2007) 41(6) Journal of Adolescent Health S51-S58.

<sup>9</sup>McGlynn C and Rackley E, 'Image-Based Sexual Abuse' (2017) 37 Oxford J Legal Stud 534, 536.

<sup>10</sup> 'General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19' (2017) 6 Int'l Hum Rts L Rev 279.

<sup>11</sup> General Recommendation No. 35 on Gender-Based Violence Against Women, Updating General Recommendation No. 19' (CEDAW, 2017).

absence of specific and uniform laws addressing TFSV at the international level remains a significant challenge in ensuring protection for victims. As TFSV often involves forms of cross-border crime, uniform laws across states are essential to ensure the protection of all individuals and provide them with the same rights.

The absence of laws poses significant challenges across multiple fronts. Without specific legal frameworks, perpetrators may exploit loopholes, evading accountability and leaving victims without adequate protection. Prosecuting such cases becomes intricate, as law enforcement struggles to gather digital evidence. Rapid technological advancements exacerbate these challenges, necessitating a proactive approach to adapt legal measures. This adaptation ensures that evidence can be collected worldwide with minimal struggle, and victims can prosecute their perpetrators based on uniform laws and definitions.

### European legal landscape

To further understand the international legal landscape of TFSV, European Union directives and regulations must be scrutinized. Directive 2011/92/EU (Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography)<sup>12</sup> is crucial for understanding child-oriented TFSV; it aims to combat child sexual abuse and exploitation and mandates EU member states to prevent the exploitation of children, including in online environments. Additionally, Directive 2000/31/EC, known as the E-commerce Directive,<sup>13</sup> outlines the liability rules for online service providers, describing the conditions under which providers may be held liable for hosted or transmitted content. Landmark cases such as *Eva Glawischnig-Piescek v Facebook Ireland Limited* (2019)<sup>14</sup> set a standard regarding the liability of hosting providers to remove illegal content and its equivalents, serving as a guiding example for future legal decisions.

Furthermore, the General Data Protection Regulation (GDPR)<sup>15</sup> outlines conditions for lawful data processing, individuals' rights regarding their data, and obligations for data controllers and processors. This regulation is crucial for providing stringent guidelines for handling personal data, allowing individuals greater control over their information, and reducing the risk of exploitation and misuse by perpetrators. In addition, by imposing accountability on data controllers and processors, the GDPR assists in safeguarding against unauthorized access and manipulation of sensitive data, mitigating the potential for data abuse.

Additionally, the EU Electronic Evidence Legislative Package (EELP), adopted in 2023, aims to facilitate the obtaining of electronic evidence across borders within the EU. However, its implementation and effectiveness remain to be seen. It introduces mechanisms for the prompt removal of TFSV content, alongside special due diligence obligations for Very Large Online Platforms

---

<sup>12</sup> (Directive 2011/92/EU of the European Parliament and of the ...) <<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF>> accessed 5 April 2024

<sup>13</sup> 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce')' (*eur-lex.europa.eu*) <<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031>> accessed 5 April 2024

<sup>14</sup> *Eva Glawischnig-Piescek v Facebook Ireland Limited*, [2019] ECLI:EU:C:2019:821.

<sup>15</sup> GDPR Portal, [gdpr-info.eu](https://gdpr-info.eu), <https://gdpr-info.eu>, accessed 5 April 2024.

(VLOPs).<sup>16</sup> As of December 2023, three of the largest porn sites have been declared as VLOPs, namely Pornhub, Stripchat, and Xvideos. VLOPs are major digital platforms that host user-generated content.<sup>17</sup> The GDPR's recognition of VLOPs and its introduction of special obligations aim to hold these platforms accountable for properly managing and removing such content, while simultaneously reducing the risk of TFSV.

## **The Netherlands**

The legislative framework in the Netherlands aims to tackle multiple aspects of TFSV by enacting laws that specifically target offenses such as grooming, non-consensual sharing of personal images, and child pornography. Article 240b of the Dutch Criminal Code criminalizes any aspect related to child pornography, including the creation and distribution of illegal content featuring children. Although Article 248e addresses grooming, this harm is only deemed illegal once the perpetrator meets with the minor, thus creating loopholes in the protection of minors against digital exploitation. Furthermore, the age of consent in the Netherlands is 16 years, rather than 18, potentially exposing a larger group of minors to exploitation.

Moreover, Article 139f of the Dutch Criminal Code criminalizes the sharing of private photos without consent, and Article 139h criminalizes revenge porn, including both its creation and distribution. However, Article 139h does not clarify whether deepfakes are included within the scope of this law. If a victim finds themselves in a situation not fully protected under the Dutch Criminal Code, they can assert their rights under the Dutch Civil Code with a claim for defamation.

In conclusion, while the combination of international, European, and Dutch laws sets a standard for combating TFSV, the legislation lacks comprehensive and uniform practices, leaving significant gaps in the protection of (still predominantly) women and girls.

### **What are the main issues?**

#### **Lack of comprehensive definitions:**

The lack of comprehensive EU definitions for the various forms of TFSV represents a significant legal deficiency. While existing laws are designed to prevent such crimes, they often lack clear definitions, creating uncertainty and making enforcement difficult. This issue is compounded by the rapid development of technology; new methods of committing TFSV are continually emerging, often outpacing precise legal definitions. One of the newer forms of TFSV, which is becoming increasingly sophisticated, is AI-generated revenge nudes/pornography.<sup>18</sup> This form currently lacks specific legislation targeting it. To address this gap, legislative frameworks must be updated with flexible definitions that can accommodate evolving technology trends.

#### **Addressing anonymous offenders:**

---

<sup>16</sup>European Commission, 'European Commission - PRESS RELEASES - Press release - European Commission proposes new rules on artificial intelligence' (Press Release, 20 February 2023) [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_2413](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413) accessed 5 April 2024.

<sup>17</sup>European Commission, 'European Commission - PRESS RELEASES - Press release - Digital Finance Package: Commission welcomes the adoption of new rules facilitating crowdfunding and online investments' (Press Release, 24 October 2023) [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_23\\_6763](https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6763) accessed 5 April 2024.

<sup>18</sup>Nudify Me: The Legal Implications of AI-Generated Revenge Porn' (15 February 2023) <https://kjk.com/2023/02/15/nudify-me-the-legal-implications-of-ai-generated-revenge-porn/> accessed 5 April 2024.

One of the biggest challenges in combating TFSV is addressing anonymous offenders who use encrypted communication methods to avoid identification. The increasing availability of encryption and anonymization software, such as Tor (the onion router), poses significant challenges for law enforcement organizations in their efforts to identify and apprehend criminals. According to reports published by Europol and Interpol,<sup>19</sup> some TFSV offenders often have advanced computer literacy, enabling them to successfully disguise their identities and alter evidence. Furthermore, international cooperation in TFSV investigations is hampered by the lack of established methods for exchanging evidence across national borders. Comprehensive solutions are required to address this issue, including updated laws, improved digital forensic tools, and international agreements to facilitate the exchange of evidence and enhance cooperation between law enforcement organizations.

### **Cross-border challenges:**

Cases of TFSV often occur across multiple national boundaries, creating difficulties for the legal system and law enforcement. The inconsistency in legal procedures and definitions among EU member states poses a challenge to effective collaboration and coordination. Different jurisdictional authorities and legal frameworks can cause delays in investigations and hinder the determination of which countries' laws apply. Moreover, issues regarding data security and privacy obstruct law enforcement authorities from sharing vital evidence. To address these obstacles, coordinated efforts are needed to harmonize legal norms and practices throughout EU member states, and to establish clear data-sharing mechanisms that prioritize privacy and efficiency. Cross-border collaboration can also be strengthened by improving technological literacy among law enforcement officers and creating specialized teams for TFSV investigations.

### **Recommendations**

#### **Develop of a Specialized TFSV Investigation Unit**

The Dutch Ministry of Justice should establish a dedicated unit for investigations of technology-facilitated sexual violence. This unit should consist of personalized trained officers and legal experts focusing specifically on TFSV cases. They should be equipped with advanced digital forensic tools, and they should be trained in sensitive ways to approach victims. Further, they should keep victims engaged and informed throughout the case and ensure they build trust to ensure that all material the victim has is provided to them. Additionally, the establishment of a specialized unit is necessary as relying on a general cybercrime unit is insufficient to address the complexities inherent in cases of TFSV, as addressed by the expert from the Centre for Sexual Violence.

#### **Implementation of an International TFSV case database**

The Netherlands should in collaboration with the European Union create a database for TFSV cases. This database should include anonymized or specific data (depending on preferences) on TFSV incidents, legal outcomes, and perpetrator profiles, which should be accessible to law enforcement agencies across the European Union.

---

<sup>19</sup>Europol and Eurojust, 'Common challenges in combating cybercrime' (June 2019) 5.

### Targeted Public Awareness Education Campaign

The Dutch Ministry of Justice and Security should launch a national public awareness campaign focusing on the dangers of TFSV, online safety, and legal repercussions for perpetrators. The campaign should include a digital literacy program aimed as an education initiative to teach students skills and knowledge necessary to safely use the digital world. The campaign should be aimed at all levels of education to ensure that students of all ages receive assistance and knowledge. The Australian government in collaboration with The Australian Institute of Family Studies has launched a study that allows them to launch campaigns and to conduct more research to ensure safety precautions against TFSV.<sup>20</sup>

In line with these efforts, the VIS project, where I worked as a project tutor; is a good example of how awareness and knowledge about TFSV can be disseminated in student communities. These initiatives further included the development of posters displayed within THUAS premises. By fostering collaboration among students from different backgrounds and leveraging various media platforms, the VIS project aimed at raising awareness about TFSV and promoting online safety practices among the respective student communities. The project envisaged a survey-informed Instagram awareness campaign (handle on Instagram being [withyoufsv](https://www.instagram.com/withyoufsv))<sup>21</sup>, which also included a podcast featuring a digital security lecturer, offering valuable insights into online safety.

### Creating a uniform system for all victim support organizations

The Netherlands, at the governmental level, should establish centers for sexual violence, with the number of centers tailored to the size of the municipality. Each center would address both physical and digital sexual violence. The overall governmental initiative should ensure that centers are open in each municipality, proportional to its size. These centers should provide comprehensive services to victims of sexual exploitation, including support in preserving evidence, legal guidance, and psychological counseling, to minimize re-victimization. Having these centers connected to the government ensures that frameworks are consistently improving, eliminating the need for each center to independently navigate the system to support victims. The centers should maintain an ongoing connection with the TFSV investigation center mentioned earlier, collaborating to ensure that evidence provided by victims is utilized efficiently and that processes advance swiftly.

### **Concluding thoughts**

In conclusion, this summary provides the highlights of the thesis, including the various issues raised by technology-facilitated sexual violence (TFSV). The recommendations aimed at strengthening the legal framework, enhancing enforcement procedures, and empowering victims of trafficking in persons (TFSV) range from the creation of specialized investigation teams to the deployment of global databases and focused publicity campaigns. As technology develops, so too must our frameworks and tactics for combating cybercrimes, guaranteeing personal safety, and encouraging a safer online community for all.

---

<sup>20</sup>‘The role of emerging communication technologies in the experiences of sexual violence’ (Australian Institute of Family Studies, accessed 5 April 2024) <https://aifs.gov.au/research/research-reports/role-emerging-communication-technologies-experiences-sexual-violence>.’

<sup>21</sup>[https://www.instagram.com/withyoufsv?utm\\_source=ig\\_web\\_button\\_share\\_sheet&igsh=ZDNIZDc0MzIxNw==](https://www.instagram.com/withyoufsv?utm_source=ig_web_button_share_sheet&igsh=ZDNIZDc0MzIxNw==)

While working on the thesis "Digital sexual crimes, accountability & adjudication in The Netherlands" for the MLR group and the VIS project, I found that focusing on both projects simultaneously was incredibly beneficial for both. The prior research I had done for my thesis helped guide the students in shaping the awareness campaign for the VIS project, ensuring that it accurately reflected the rights, responsibilities, and avenues for recourse for the target audience in the Netherlands. The multi-level regulation framework proved to be very helpful in understanding and interpreting the legal TFSV landscape. The thesis findings not only aided in informing academic discourse but also directly impacted practical initiatives like the VIS project. Being a part of the VIS team while conducting research on a similar topic allowed for the students of the VIS project to have extra feedback specifically for their literature review and receiving guidance for their research within the Netherlands.

In reflecting on my work with both the VIS project and the thesis, I have not only discovered a topic of great interest to me that has ignited my desire to help solve the aforementioned issues in the future, but I have also developed a passion for teaching and building connections with students, fostering a sense of community. Both the VIS project and the thesis have been a new and exciting process and they are both accomplishments I will look back on with great satisfaction. I thank both Dr. Matczak for this opportunity and the MLR group.