


ARTICLE

Special Issue: Sexual Violence and Criminal Justice in the 21st Century  
Section II: Sexual Autonomy and the Limits of Criminal Law

# Sexual Violence in the Digital Age: A Criminal Law Conundrum?

Olga Jurasz<sup>1</sup> and Kim Barker<sup>2</sup> 

<sup>1</sup>Senior Lecturer, Open University Law School, Milton Keynes, United Kingdom and <sup>2</sup>Senior Lecturer, Open University Law School, Milton Keynes, United Kingdom

Corresponding author: [kim.barker@open.ac.uk](mailto:kim.barker@open.ac.uk)

(Received 05 July 2021; accepted 05 July 2021)

## Abstract

The emergence of new interactions, notably those online, has led to the parallel development of criminal behaviors—not all of which are captured by the current legal framework. This article addresses the challenge posed to criminal law by the emergence of technologically facilitated violence, specifically its sexualized online forms. In particular, it argues for cautious yet specific criminalization of violent behaviors online whilst considering the broader criminal liabilities of all actors involved in the facilitation and perpetration of digital sexual violence. This article draws upon national—contentious—examples of attempts to regulate disruptive sexual violence perpetrated through digital means, with particular attention given to provisions in the UK, Germany, and France.

**Keywords:** Digital violence; sexual violence; criminal law; OTFSV; IBSA; TBSA

## A. Introduction: Digital Abuse and Criminal Law After #MeToo

The #MeToo movement has highlighted—on a global and public scale—the common and widespread nature of sexual violence against women worldwide. In doing so, the movement has not unearthed anything new. As such, the ‘war on women’<sup>1</sup> exemplified through everyday sexual and gender-based violence as well as ‘extraordinary’ violence, has been documented, reported and critiqued for decades, especially by feminist scholars and activists.<sup>2</sup> However, #MeToo has powerfully changed the way in which conversations about sexual violence against women are taking place, becoming an example of digital feminist activism.<sup>3</sup> From being a topic surrounded by stigma, it has evolved into a publicly acknowledged and universally spoken about subject, marking a

<sup>1</sup>See SUE LLOYD-ROBERTS, *THE WAR ON WOMEN AND THE BRAVE ONES THAT FIGHT BACK* (2016).

<sup>2</sup>See, e.g., CAROL SMART, *FEMINISM AND THE POWER OF LAW* (1989); see also LIZ KELLY, *SURVIVING SEXUAL VIOLENCE* (1988); ALEXANDRA STIGLMEYER, *MASS RAPE: THE WAR AGAINST WOMEN IN BOSNIA-HERZEGOVINA* (Marion Faber, trans., 1994); NOËLLE QUÉNIVET, *SEXUAL OFFENSES IN ARMED CONFLICT & INTERNATIONAL LAW* (2005); ANASTASIA POWELL & NICOLA HENRY, *SEXUAL VIOLENCE IN A DIGITAL AGE* (2017); KIM BARKER & OLGA JURASZ, *ONLINE MISOGYNY AS A HATE CRIME: A CHALLENGE FOR LEGAL REGULATION?* (2019).

<sup>3</sup>For an in-depth analysis of the #MeToo movement, see KAREN BOYLE, *#MeToo, WEINSTEIN AND FEMINISM* (2019). That said, #MeToo has also been criticized for not capturing the daily, structural violence and harassment experienced by marginalized groups of women, such as Dalit women in India. See Poorvi Gupta, *Seeing #MeToo Narrative from the Lens of Marginalized Communities*, SHE THE PEOPLE TV (Oct. 11, 2018), <https://www.shethepeople.tv/top-stories/issues/metoo-narrative-marginalized-communities>.

significant shift in the public understanding of and appreciation for the magnitude of sexual violence against women and its effect on the survivors. Importantly, the rise of #MeToo has also invited questions about the power of law, structural violence and institutionalized sexism vis-a-vis the harrowing experiences of women subjected to sexual violence. In doing so, it led—albeit perhaps not intentionally—to questioning the role, deficiencies, and inherent bias of criminal law in addressing sexual violence and providing an effective remedy to the victims.

Taking the momentum of the #MeToo movement as a point of departure, this article considers the scope and limitations of criminal law in addressing a modern phenomenon of digital sexual violence. Throughout the article, we use the terminology of ‘digital sexual violence’ and ‘online technologically facilitated sexual violence’ (OTFSV) interchangeably to signify the changing nature of terminology used in literature as well as law and policy instruments to describe this issue. Terms ‘violence’ and ‘abuse’ are used synonymously, reflecting the diverse range of terms used to describe online abusive behaviors,<sup>4</sup> while also highlighting one of the complexities in this area given the absence of agreed-upon terminology. Online harassment is used to describe the use of communications technologies to harass, control, and abuse someone, including unsolicited and threatening behaviors.<sup>5</sup> In our analysis, we particularly focus on non-image-based forms of digital sexual violence—such as, for example, sexually explicit tweets or Facebook messages—which we refer to as text-based sexual abuse (TBSA).<sup>6</sup> Sexual violence—here, in its online/ digital forms—is viewed as a form of gender-based violence.<sup>7</sup>

The analysis presented here raises questions about the suitability of existing criminal law in addressing OTFSV, noting the conceptual and pragmatic obstacles to doing so. The core argument advanced in this article is that a meaningful criminal law reform is an important and much needed step in facilitating accountability for OTFSV, but it has significant limitations in terms of preventing such abuse from reoccurring in the future. As such, whilst we argue that criminal law reform is necessary to achieve symbolic justice for victims of digital sexual violence and to subvert the normalization of sexual and gender-based abuse of women, it is essential that such reform is accompanied by parallel developments in other areas of the law as well as long-term measures aimed at changing social attitudes towards violence against women—both online and offline.

## B. Sexual Violence in Online Environments

The explosion in online time, and in internet use for work, social purposes, communications, and information, has offered significant potential for new interactions, and new modes of engagement. Newer, and more interactive digital and online spaces offer opportunities that have previously never been replicable in virtual contexts. For each development of online environments, increasingly prevalent concerns surrounding the behaviors that such spaces encourage, foster, and fail to prevent abound. This is, in part, because each of these digital spaces replicates in some way the human interactions which occur outside of online environments, for predictable reasons—as noted by Castronova:

<sup>4</sup>For the authors’ critique of the linguistic fragmentation regarding terms used to describe various acts of online technologically facilitated violence against women, see Kim Barker & Olga Jurasz, *Online Violence Against Women as an Obstacle to Gender Equality: a Critical View from Europe*, 1 EUR. EQUAL. L. REV. 47 (2020).

<sup>5</sup>See Eur. Inst. for Gender Equal., *Cyber Violence Against Women and Girls* (June 23, 2017), <https://eige.europa.eu/publications/cyber-violence-against-women-and-girls>.

<sup>6</sup>The term text-based abuse (TBA) was coined by the authors and introduced in our book. See KIM BARKER & OLGA JURASZ, *supra* note 2. For a more in-depth discussion of text-based sexual abuse, see Kim Barker & Olga Jurasz, *Text-based (Sexual) Abuse and Online Violence Against Women: Towards Law Reform?*, in TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE – INTERNATIONAL PERSPECTIVES AND EXPERIENCES 247–64 (Jane Bailey et al. eds., 2021).

<sup>7</sup>However, not all forms of gender-based violence are sexualized in nature.

Everything that happens in a synthetic world is the consequence of the interaction of human minds, and our minds have things like Love, Property, Justice, Profit, War and Exploration hard-wired into them. We could not create a world and put people in it without also enabling sex, trade, and battle.<sup>8</sup>

The replicability of norms that occurs in the development of online environments presents additional challenges because while these online environments are designed to allow us to do things differently to the offline, they are also, at least partially, designed to replicate those offline things. The somewhat mixed messaging about the role and purpose of different online environments therefore poses problems that have been witnessed throughout the development of the Internet. These are evident at every milestone; from the origins of email messages leading to incredible levels of spam, to the first social media post leading to online violence, online hate, and online text-based abuse, to the use of video calling leading to ‘zoom-bombing’ difficulties. The boom that developments in technology has offered, has unfortunately been mirrored through a rapid explosion in the use of the Internet for criminal activities, most of which have not been adequately captured by the criminal law because technology has, of course, outpaced both law reform, and legal conceptualizations of online harms, and digital violence. In online environments, particularly, multi-user platforms such as social media sites and online games, this criminality has increasingly focused on sexual and violent elements.

The trajectory of technological capability has consequently been matched by the manipulation of technology for the purposes of sexual violence, including digital sexual violence in online environments. While the rise in digital sexual violence is worthy of comment, not least because it is in many respects a digital—and sexualized—pandemic, the portrayal/characterization of physical acts captured by the umbrella of digital sexual violence resembles those experienced in offline situations. Acts such as the making/sending of sexualized threats including rape, harassment,<sup>9</sup> assault, image-based abuses,<sup>10</sup> and digital sexual violations<sup>11</sup> are all behaviors which are increasingly prominent, and which fall within the purview of digital sexual violence, not just as behaviors requiring criminal regulation, but as actions which prove increasingly challenging for the criminal justice system to address in the twenty-first century. The challenge for the criminal law in attempting to address sexual violence in online environments is compounded due in part to the lack of suitability of current legal provisions, but also due to the rapidly rising, and evolving forms of behavior that require effective understanding from—and by—law enforcement bodies, and judicial organizations.<sup>12</sup>

Insights from recipients of digital sexual violence highlight that, “[i]t happens to all women so it’s almost not worth mentioning as it’s so unremarkable.”<sup>13</sup> This ‘normalization’<sup>14</sup> stems from the origins of online multi-user environments, and the manners in which behaviors in online spaces were regarded as ‘just online’ therefore not really a problem, nor worthy of regulation. The ‘acceptability’ within some online environments of sexual violence is something which has long been suggested as a ‘get-out’ from discussions surrounding online interactions.<sup>15</sup> The ‘online’ versus ‘offline’ debate relies on the notion that there should be different conceptions of acceptability of behaviors depending on whether the behavior is being conducted in the online

<sup>8</sup>EDWARD CASTRONOVA, *SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES* 42 (2006).

<sup>9</sup>KIM BARKER & OLGA JURASZ, *supra* note 2, at 68–70; Kim Barker & Olga Jurasz, *supra* note 6.

<sup>10</sup>Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 OXFORD J. LEGAL STUD. 534 (2017).

<sup>11</sup>CARRIE GOLDBERG, *NOBODY’S VICTIM: FIGHTING PSYCHOS, STALKERS, PERVS, AND TROLLS* (2019).

<sup>12</sup>See Kim Barker & Olga Jurasz, *supra* note 4.

<sup>13</sup>Ruth Lewis, Michael Rowe & Clare Wiper, *Online Abuse of Feminists as an Emerging Form of Violence Against Women and Girls*, 57 THE BRIT. J. CRIM. 1462, 1474 (2017).

<sup>14</sup>Kim Barker & Olga Jurasz, *Online Misogyny: A Challenge for Global Feminism?*, 72 J. INT’L AFF. 95, 97 (2019).

<sup>15</sup>There is a prominent counter opinion proffered repeatedly in discussions surrounding digital sexual violence, and online violence against women & girls (OAVW), that this is not a problem because it is all “online.”

environment—the so-called ‘real life’ divide. This is a flawed distinction. Although the physical act of sexual violence, and the degree of violation of sexual autonomy that arises from it, differ between online and offline worlds, both acts share the root causes that motivate such behaviors in the first place: patriarchy, gender inequality, discrimination against women. Therefore, not only does this division no longer have a realistic foundation—especially in light of numerous, and repeated efforts to regulate online platforms and behaviors<sup>16</sup>—but it also highlights the challenges in addressing sexual and digital sexual violence.

### I. Evolving Digital Violence—The Origins

Digital violence, even in the twenty-first century’s more nuanced forms, is not a new phenomenon. It has existed since the origins of the internet, and especially since the first multi-user online spaces. The earliest reports of digital violence are not necessarily captured as digital sexualized violence, but nonetheless, the origins rest firmly in the male-dominated environments of the early online games. One of the earliest reports of digital sexualized violence is the rape of a game character in *LambdaMOO* in the early 1990s.<sup>17</sup> This, while one of the most high-profile, has tended to receive comment as an instance of internet regulation, rather than as a criminal act. Nonetheless, it is one of the examples of how early online violence adopted a sexualized element, albeit one which went unacknowledged and unchallenged by law enforcement and regulatory bodies. The manner in which virtual characters subject one another to violations—alleged to be virtual rapes—illustrates the difficulties in early discussions surrounding how to address such behavior. In 1993, this was addressed as a user issue within the game itself, rather than one involving a criminal complaint—although with some suggestion that, at best, the actions relate to simulation and nothing more harmful—relating to the virtual world in which the sexualized violence occurred. This is not the only, early, example of a situation where claims of digital sexual violence are conceptualized. In 2007, a further high-profile allegation relating to rape claims in a virtual environment was reported to the Belgian Police.<sup>18</sup>

A narrow conceptualization of such alleged behavior may infer that there can be no rape of a virtual character which consists of little more than software code, but instead, the conduct complained of amounts to harassment with sexualized undertones in a digital environment. Making such narrow categorizations is tantamount to the dismissal of the broader context and root causes of such behaviors, but also the dismissal of the potential harms which may have been inflicted by virtue of the behavior in the online environment. More than this though, such an example highlights some of the difficulties that arise when incidents such as this are reported in the public domain—discussions which question whether it is even possible for digital violence, and digital sexual violence to occur.<sup>19</sup> Fortunately, debates, awareness, and understandings have developed since the reports of the 1990s and mid-2000s, albeit they remain far from adequate for addressing such issues, and the more developed forms of digital sexual violence. The criminal law was

<sup>16</sup>For instance, the UK Government is committed to introducing internet safety laws through proposed Online Harms legislation. See HM GOVERNMENT, ONLINE HARMS WHITE PAPER: FULL GOVERNMENT RESPONSE TO THE CONSULTATION, 2020, [Cmd.] 354 (UK). Meanwhile, the EU has released its much awaited Digital Safety Act draft legislation. See *Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and Amending Directive (EC) 2000/31, COM (2020) 825 final* (Dec. 15, 2020).

<sup>17</sup>See Julian Dibbell, *A Rape in Cyberspace (Or TINY SOCIETY and How to Make One)*, in, VIOLATION: RAPE IN GAMING 21–44 (Clarisse Thorn & Julian Dibbell eds., 2012). See also Kim Barker & Olga Jurasz, *Gender, Human Rights and Cybercrime: Are Virtual Worlds really that Different?*, in LAW AND POPULAR CULTURE: INTERNATIONAL PERSPECTIVES 79, 83 (Michael Asimow, Kathryn Brown, & David Ray Papke eds. 2014).

<sup>18</sup>See Kim Barker & Olga Jurasz, *supra* note 17, at 79 & 83; see also Benjamin Duranske, *Reader Roundtable: Virtual Rape Claim Brings Belgian Police to Second Life*, VIRTUALLY BLIND (Apr. 24, 2007), <http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/>.

<sup>19</sup>It should be noted that some of these difficulties reflect a lack of willingness to recognize such behaviors as problematic, particularly by those immersed in online subcultures, and those who have chosen to withdraw from “real” (offline) life. See DAVID BELL, AN INTRODUCTION TO CYBERCULTURES 175 (2003).

unprepared for instances of digital and virtual sexual violence in the 1990s, but the regulatory and enforcement challenges continue to grow as new forms of digital sexual violence emerge.

## II. *Virtual Black Eyes & Sexualized Threats: Normalizing Sexism Online*

The shifting forms of digital sexual violence, moving towards OTFSV, and occurring in greater numbers across a multitude of platforms has been a matter of concern for the regulatory framework—both criminal, and internet—since the mid-2000s. Most notably, the modes of OTFSV have developed and become more sophisticated at the same time as technology has exposed greater numbers of people to such behaviors and harms.

Some early examples of digital sexual violence originate with the founders of one of what are now the ‘Internet Giants.’ One of the most notable is the ‘FaceMash’ website that was developed by Facebook creator Mark Zuckerberg in 2003. The website was designed to allow women to be pitted against one another, or farm animals, in a competition to see which would be voted as the most attractive<sup>20</sup> and serves as just one example, albeit one which developed into something more menacing, of the ways in which gender stereotypes and tropes play out in online spheres. This modified version of FaceMash’s inspiration, Hot or Not,<sup>21</sup> embodied within it a much nastier, vitriolic element of direct comparisons in the public domain. Originally suggested as more prank<sup>22</sup> than anything else, Zuckerberg claims to have not contemplated that this could give rise to and what is now a more broadly recognized phenomenon, online & digital bullying. In initiating FaceMash, this website arguably marks the emergence of image-based harassment, and highlights what is now one of the forms of digital sexualized harassment online. By creating the means to mine for images of women, and publicly share those images on a website, the predecessor to image based sexual abuse was conceived. It is not surprising that the successor to Zuckerberg’s FaceMash—Facebook—while being one of the leading social media platforms, is, more alarmingly, the one reporting the highest numbers of OTFSV incidents.<sup>23</sup> The FaceMash example is followed by two much more severe, and extreme examples, both of which highlight on a global scale the graphic digital sexualized violence sent to women. First, the “Beat Up Anita Sarkeesian Game,” and second, “Zoe Quinn & Gamergate.”

The first example is the game that was created by Bendilin Spurr, which allows users to virtually beat-up Anita Sarkeesian:

Anita Sarkeesian has not only scammed thousands of people out of over \$160,000, but also uses the excuse that she is a woman to get away with whatever she damn well pleases. Any form of constructive criticism, even from fellow women, is either ignored or labeled to be sexist against her.

She claims to want gender equality in video games, but in reality, *she just wants to use the fact that she was born with a vagina to get free money and sympathy from everyone who crosses her path.*<sup>24</sup>

<sup>20</sup>See STEVEN LEVY, *FACEBOOK: THE INSIDE STORY* 48–49 (2020).

<sup>21</sup>Operating on a similar basis, but rather than ranking women in comparisons, required a ranking of 1–10 in attractiveness.

<sup>22</sup>See Steve Annear, *A Congressman Asked Mark Zuckerberg if ‘Facemash’ Was Still Up and Running*, *BOSTON GLOBE* (Apr. 12, 2018), <https://www.bostonglobe.com/metro/2018/04/12/congressman-asked-mark-zuckerberg-facemash-was-still-and-running-online/IBtqskC771xtkLf6QcQrzL/story.html>.

<sup>23</sup>See *Free to Be Online? Girls’ and Young Women’s Experiences of Online Harassment*, PLAN INTERNATIONAL, <https://plan-international.org/publications/freetobeonline> (last visited June 6, 2021); see also Melissa Davey, *Online Violence Against Women ‘Flourishing’ and Most Common on Facebook, Survey Finds*, *THE GUARDIAN* (Oct. 4, 2020), <https://www.theguardian.com/society/2020/oct/05/online-violence-against-women-flourishing-and-most-common-on-facebook-survey-finds>.

<sup>24</sup>Sheena Lyonais, *Toronto Tweeter Causes Uproar Over Violent “Beat Up Anita Saarkesian” Game*, *TORONTO STANDARD* (Jul. 9, 2012), <http://www.torontostandard.com/industry/toronto-tweeter-causes-twitter-uproar-over-violent-beat-up-anita-sarkeesian-game/> (emphasis added).

Sarkeesian became the object of Spurr's game for campaigning to develop a video series deconstructing stereotypes of women and female game characters. The game description makes it abundantly clear that there is a significant sexualized element to it. The game was designed to allow users to click on an image of Sarkeesian and replicate virtually, punching her in the face, causing bruising, and lesions to appear on the image. The entire point of the game was to punch a woman in the face, "for having an opinion."<sup>25</sup> Sarkeesian herself notes that the culture of sexism is rewarded, with women being subject to increasing forms of silencing online:

[W]hether it is a cyber mob or just a handful of hateful comments, the end result is maintaining and reinforcing and normalizing a culture of sexism, where men who harass are supported by their peers and rewarded for their sexist attitudes and behaviors where women are silenced, marginalized and excluded from full participation.<sup>26</sup>

The second example highlights a different element to OTFSV and focuses on the severity of threats and abuse sent to women, via digital and online means, in what is now known as Gamergate.<sup>27</sup> The origins of Gamergate rest in behaviors which could generously, albeit dismissively, be described as online bullying. These behaviors are much more severe and include threats of physical harm including rape and murder, and are described by the woman at the center of Gamergate, as the destruction of her life.<sup>28</sup> The trigger for Gamergate was game developer Zoe Quinn's efforts in producing and developing the online game *Depression Quest*.<sup>29</sup> The *New Yorker* infers that the reason for the volume of abuse and seriousness of the threats against Quinn—severe enough to make her leave her home<sup>30</sup>—is related to the quality of the game she developed,<sup>31</sup> but others are less convinced and suggest that the trigger is the fact that she is a woman.<sup>32</sup>

Regardless of the reason for the motivation, the resulting behaviors and targeting of Quinn escalated when her ex-boyfriend wrote a series of blog posts indicating that she had cheated on him with other game industry workers. The backlash within gaming circles intensified and these allegations became almost unopposable truths. The ultimate result was not only intensified digital and sexualized threats in the form of rape, and assault, but also the public sharing of her address and phone number online<sup>33</sup> so that these threats could potentially be carried out. In publicly sharing these details, the effect of the threats upon the victim is heightened, not because of the potential criminality, but rather because of the reach of online information which infers the potential of physical harm by persons unknown at times unknown. By making threats and sharing contact details, the stranger danger, and the unknown of whether these threats will lead to physical harm adds in itself greater psychological effects to the recipient of such communications. The emergence of violence in online environments has given rise to a new, and significant

<sup>25</sup>*Id.*

<sup>26</sup>Anita Sarkeesian, *TedXWomen Talk "Online Harassment and Cyber Mobs"*, FEMINIST FREQUENCY (Dec. 5, 2012), <https://feministfrequency.com/video/tedxwomen-talk-on-sexist-harassment-cyber-mobs/>.

<sup>27</sup>See Helen Lewis, *Gamergate a Brief History of a Computer-age War*, THE GUARDIAN (Jan. 11, 2015), <https://www.theguardian.com/technology/2015/jan/11/gamergate-a-brief-history-of-a-computer-age-war>; see also *The Guardian View on Gamergate: When Hatred Escaped*, THE GUARDIAN (Aug. 20, 2019), <https://www.theguardian.com/commentisfree/2019/aug/20/the-guardian-view-on-gamergate-when-hatred-escaped>.

<sup>28</sup>See ZOE QUINN, CRASH OVERRIDE: HOW GAMERGATE (NEARLY) DESTROYED MY LIFE AND HOW WE CAN WIN THE FIGHT AGAINST ONLINE HATE (2017).

<sup>29</sup>See *Depression Quest* <http://www.depressionquest.com/> (last visited June 6, 2021).

<sup>30</sup>This impact, for example, the social and familial harm in being forced to leave home for the sake of personal safety, is something that is growing in recognition, albeit not per se by the criminal law. See Kim Barker & Olga Jurasz, *supra* note 6.

<sup>31</sup>See Simon Parkin, *Zoe Quinn's Depression Quest*, THE NEW YORKER (Sept. 9, 2014), <https://www.newyorker.com/tech/annals-of-technology/zoe-quinn-depression-quest>.

<sup>32</sup>See Jay Hathaway, *What Is Gamergate, and Why? An Explainer for Non-Geeks*, GAWKER (Oct. 10, 2014), <https://gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080>.

<sup>33</sup>In essence, doxing.

phenomenon of digital sexualized violence—one which manifests itself much more widely across the internet, but which emphasizes text-based sexual abuse (TBSA) and image-based sexual abuse (IBSA), and yet, such a phenomenon is not equally addressed by the criminal law. Specific legal provisions have been introduced to capture IBSA, and yet TBSA, despite its harms, remains at worst, almost unregulated, and at best, sporadically made to “fit” within non-specific legal provisions.

### III. Sexual Abuses Online— IBSA & TBSA

The prominence of OTFSV is a hangover from a prolonged failure to address earlier behaviors and problems in online environments. The lack of criminal law responses to complaints of issues in online environments in the 1990s, early 2000s, and early 2010s demonstrates persistent failures to tackle the problem, which is now a phenomenon with wide-ranging impact.

In the last decade, digital sexual violence has developed still further, and evolved from the specific game-based violence seen in the 2000s. In particular, two examples indicate the evolution and scale of the challenge facing the criminal law. First, the development of image-based harassment into IBSA including other, associated forms of image harassment,<sup>34</sup> such as upskirting, downblousing, sextortion, and deepfakes.<sup>35</sup> Second, the evolution of threats into text-based sexual abuses. These forms of OTFSV are all direct descendants from earlier problems, arguably facilitated and encouraged by the lack of appropriate responses by the legal system.

IBSA, also known as “revenge pornography,”<sup>36</sup> has also seen a significant rise to prominence. The unauthorized and non-consensual dissemination of intimate images shares characteristics of behaviors seen earlier. In the non-consensual sharing element of for example, FaceMash, but with a much more sinister element that has also some shared origins in the allegations that triggered the backlash and online harassment of Zoe Quinn. The non-consensual sharing of intimate images has at its heart the capturing of the criminal sharing of nude or sexual photographs. Often these are taken when relationships are good, and disseminated in the pursuit of revenge, or destruction of reputation once things turn sour. The sexualized element is central to the harm, and to the sharing behavior that follows. Sharing images non-consensually that were never intended for public viewing is at the heart of the offence here. This form of OTFSV has unusually seen a relatively rapid rise in legislation from the criminal justice system,<sup>37</sup> with criminalization and prosecutions being swiftly pursued. Such a response is, partially, because the ‘harmful’ aspect of images is easier to capture, and to categorize, particularly because in England & Wales a core element of the criminal offence is the *causing* of distress to the person depicted in the image.<sup>38</sup> It is unfortunate that similar distress has not yet been captured in legislation for non-image-based forms of OTFSV.

TBSA meanwhile refers specifically to the manner in which rape threats, and physical assault threats are communicated through online platforms. It is defined here as:

<sup>34</sup>See Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell & Adrian J. Scott, *IMAGE-BASED SEXUAL ABUSE: A STUDY ON THE CAUSES AND CONSEQUENCES OF NON-CONSENSUAL NUDE OR SEXUAL IMAGERY* (2020).

<sup>35</sup>See Kirsti Melville, *The Insidious Rise of Deepfake Porn Videos – and One Woman Who Won’t Be Silenced*, ABC NEWS (Aug. 29, 2019), <https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774>.

<sup>36</sup>Clare McGlynn & Erika Rackley, *supra* note 10.

<sup>37</sup>Image-based sexual abuse is now regulated by law across the UK. For England & Wales, Scotland, and Northern Ireland. See Criminal Justice and Courts Act 2015 § 33 (UK); Abusive Behavior and Sexual Harm (Scotland) Act 2016 (asp 22) § 2; Justice Act (Northern Ireland) 2016, §§ 51–53.

<sup>38</sup>See *Revenge Pornography – Guidelines on Prosecuting the Offence of Disclosing Private Sexual Photographs and Films*, CROWN PROSECUTION SERVICE (CPS) (Jan. 24, 2017), <https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-prosecuting-offence-disclosing-private-sexual>.

[W]ritten, electronic communication containing threatening and/or disruptive and/or distressing content such as e.g., textual threats to kill,<sup>39</sup> rape or otherwise inflict harm on the recipient of such messages.<sup>40</sup>

This form of OTFSV includes threats made to women in prominent positions and public life, especially elected officials.<sup>41</sup> It is particularly troubling that this form of OTFSV is often overlooked by the criminal law as being “just” a communications misuse offence,<sup>42</sup> rather than a form of digitalized sexualized violence, especially where studies suggest that thirty percent of women have experienced such forms of OTFSV at least once.<sup>43</sup> The prevalence of this issue cannot be overlooked as it has tended to be previously. Often short messages on social media are not captured within the criminal law framework, and where they are, they are not prosecuted on the basis of having a sexualized element to the violence. In rare instances, consideration is given to the types of threat made—but this is unusual.<sup>44</sup> It is particularly harmful for women choosing to express opinions on social media and online environments—high profile examples indicate this. For instance, the first black Member of Parliament in the United Kingdom, Diane Abbott, was targeted with more than 8000 tweets in the first six months of 2017 alone.<sup>45</sup> This is not an isolated incident, with other prominent women also being subjected to similar levels of OTFSV communications which are threatening and abusive.<sup>46</sup>

#### IV. The Rise of OTFSV as a Challenge for the Criminal Law?

What the examples illustrate, beyond the evolution of digital sexual violence, is the vitriolic nature of OTFSV, and the significant volumes of it. The nature, form, and scale of OTFSV has not yet been adequately captured in the criminal law system. Significantly, the harmful nature and profound influence of OTFSV has been overlooked by the legal frameworks, not least when it comes to TBSA. The criminal law conceptions of harm tend to rest—because communications which have traditionally been placed within communications misuse rather than sexual violence offences—on notions of distress, and offensiveness.<sup>47</sup> This conceptualization overlooks the personalized influence upon recipients of such violence.<sup>48</sup> For instance, Zoe Quinn encountered harms that the criminal law framework does not necessarily recognize—she had to leave her

<sup>39</sup>Textual threats to kill are not per se sexual in nature. However, it is common that such treats are accompanied by threats of sexual violence, e.g. ‘I’ll rape and kill you.’

<sup>40</sup>KIM BARKER & OLGA JURASZ, *supra* note 2.

<sup>41</sup>See Kim Barker & Olga Jurasz, *Gendered Misinformation & Online Violence Against Women in Politics*, CO-INFORM (Mar. 2020), <https://coinform.eu/gendered-misinformation-online-violence-against-women-in-politics-capturing-legal-responsibility/>. See also Kim Barker & Olga Jurasz, *supra* note 4, at 50.

<sup>42</sup>See further discussion below at C.I: Criminal law: OTFSV and digital harms.

<sup>43</sup>See European Union Agency for Fundamental Rights, *Violence Against Women: an EU Wide Survey. Main Results Report*, FRA (Mar. 5, 2014), <https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>.

<sup>44</sup>See, e.g., Judge Howard Riddle, Commentary, *R v. Nimmo & Sorley (2014) (Unreported) Sentencing Remarks* (Jan. 24, 2014), <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-v-nimmo-and-sorley.pdf>.

<sup>45</sup>See #ToxicTwitter: *Violence and Abuse Against Women Online*, AMNESTY INTERNATIONAL (2018), <https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/>; see also Azmina Dhrodia, *Unsocial Media: Tracking Twitter Abuse Against Women MPs*, MEDIUM (Sept. 3, 2017), <https://medium.com/@AmnestyInsights/unsocial-media-tracking-twitter-abuse-against-women-mps-fc28aeca498a>.

<sup>46</sup>See Kim Barker & Olga Jurasz, *supra* note 14, at 97.

<sup>47</sup>See Judge Howard Riddle, Commentary, *R v. Nimmo & Sorley (2014) (Unreported) Sentencing Remarks* (Jan. 24, 2014), <https://www.judiciary.uk/wp-content/uploads/JCO/Documents/Judgments/r-v-nimmo-and-sorley.pdf>. See also Commentary, *R v. Viscount St Davids (2017) (Unreported) Sentencing Comments* (Jul. 13, 2017), <https://www.judiciary.uk/wp-content/uploads/2017/07/r-v-lord-st-davids-20170714-sentencing-remarks.pdf>.

<sup>48</sup>See Kim Barker & Olga Jurasz, *supra* note 6, at 247–64.



home, and seek alternate accommodation. Similarly, in other instances, economic, social, as well as psychological harms have all been the result of profound and prolific OTFSV.<sup>49</sup> These harms are not currently captured within the legal framework and by overlooking such harms, there is a significant void within the regulatory provisions which require ‘joined up thinking’<sup>50</sup> from perspectives beyond criminal law.

It is nevertheless possible to identify three factors which mark out the damage that sexual violence in online environments can inflict that pose challenges for the criminal law. First, the rapidity with which digital sexual violence and OTFSV has risen to prominence; second, the lack of understanding and uniformity of approach in addressing digital crimes incorporating sexual violence; and third, the impact of such behaviors on the recipients and victims.

### C. OTFSV and the Limits of Criminal Law

OTFSV poses a challenge to legal regulation, particularly ensuring the criminal accountability of the perpetrators, on several levels. There is no supranational criminal law which addresses the issue of OTFSV—rather, legislating for and prosecuting these forms of sexual violence lies at a discretion of individual states. This leads to a fragmented approach amongst states in terms of establishing accountability for OTFSV—an issue which is further complicated by the potential of these offences to be committed extraterritorially. Furthermore, gaps in legislation, the lack of appreciation of the full extent of harms caused by OTFSV, a common misperception that digital and online forms of violence—especially those on social media—are less serious than crimes of violence happening offline,<sup>51</sup> and the competing priorities of the justice system contribute to the problematic status quo in addressing OTFSV.

#### I. Criminal Law, OTFSV and Digital Harms

First and foremost, there are significant deficiencies in the way that criminal law conceptualizes OTFSV—and digital forms of violence more generally. Whilst harms arising from such forms of violence are gradually being acknowledged and discussed, both in the academic and law & policy making contexts,<sup>52</sup> the law lags behind the debates. Criminal law, and the criminal justice system have been slow in responding to the rise in OTFSV. That said, some forms of OTFSV, such as image-based sexual abuse (IBSA) and voyeurism, have been the subject of a speedy law reform in many countries across the world.<sup>53</sup> In contrast, TBSA has not gained an equivalent level of

<sup>49</sup>See *Id.*

<sup>50</sup>Kim Barker & Olga Jurasz, *supra* note 4, at 58.

<sup>51</sup>See Kim Barker & Olga Jurasz, *supra* note 6, at 247, 254–60; *Met Chief Cressida Dick Backs ‘Traditional’ Policing Call*, BBC NEWS (Nov. 2, 2018), <https://www.bbc.co.uk/news/uk-46068013>.

<sup>52</sup>For instance, at the time of writing, there are ongoing consultations concerning online harms legislation in the UK and in Australia. At an international level, the UN Special Rapporteur on Violence Against Women, Its Causes and Consequences, called for evidence on the issue of OVAW in 2017. For authors’ submission, see Kim Barker & Olga Jurasz, *Submission of Evidence on Online Violence Against Women to UN Special Rapporteur Violence Against Women, Its Causes and Consequences, Dr Dubravka Šimonović*, THE OPEN UNIVERSITY (2017), <http://oro.open.ac.uk/52611/>. Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), a body overseeing states’ compliance with international obligations enshrined in the Istanbul Convention is due to issue its first General Recommendation on the topic of online and technologically facilitated violence against women and girls, as of December 2020.

<sup>53</sup>See e.g. Loi 2016–1321 du 28 Septembre 2015 Project de loi pour une République numérique [Law 2016–1321 of September 28, 2015 on Digital Republic Law] (Fr.); Prevention of Sexual Harassment Law, 5758–1998, SH 5758, as amended (Isr.); see also Canada Criminal Code, R.S.C. 1985, c C-46, s. 162.1 (amended through Bill C-13 Protecting Canadians from Online Harm Act 2015) (Can.). See also Shiji Seiteki Gazou Kiroku No Teikyotō Niyoru Higai No Boushi Nikansuru Hōritsu [Act on Prevention of Victimization Resulting from Provision of Private Sexual Image], Law No. 126 of 2014 (Japan); Criminal Justice and Courts Act 2015, § 33 (Eng. & Wales); Abusive Behaviour and Sexual Harm Act 2016, Part 1, § 2 (Scot.); see also Justice Act 2016, Part 3 § 51 (N. Ir.); Kim Barker & Olga Jurasz, *supra* note 6, at 247, 250–51.

recognition in the legal systems. As such, there is generally an absence of specific legal provisions dealing with these forms of sexual violence, with possibly a notable exception of IBSA provisions. This leaves non-image-based forms of TFSV largely undefined in law and, what follows, legally/criminally unaccounted for.

Other laws may serve as the basis for prosecuting online conduct involving TFSV—such as, for instance, provisions concerning threats, stalking or harassment, and communications offences.<sup>54</sup> Although TFSV may indeed fall under these provisions, the act of TFSV would then need to satisfy the *actus reus* and *mens rea* for that particular offence, including different evidential thresholds. Given varying thresholds for these offences, this in turn leads to a highly fragmented and inconsistent approach to prosecuting TFSV which is likely to severely restrict the avenues of redress for the victims.

A further complicating factor is posed by the contextual aspect of the TFSV. Namely, that they largely take place in the online sphere. Although, as we argue elsewhere,<sup>55</sup> the online nature of the offences *per se* is not an obstacle in ensuring criminal accountability for TFSV, it is proving problematic when it comes to consideration of TFSV due to the way in which underlying offences are characterized in law. For instance, some of the existing criminal law provisions in England & Wales—which, in principle could apply to cases involving online TFSV—tend to focus on concepts such as ‘proximity’ or ‘hearing’ which prove redundant in the context of acts taking place in the online sphere, especially on social media. This can be illustrated by section 4(1) of the Public Order Act 1986, amended in 2006, which makes it an offence to use threatening, abusive, or insulting words or behavior, or to display to another person any writing or visible representation which itself is threatening, abusive, or insulting with the intention of causing the person to whom threats are made to believe that, “immediate unlawful violence will be used against him” or “to provoke the immediate use of unlawful violence by that person.” The overreliance on the notions of physical proximity, immediacy or provocation of violence, as well as requirement that the threat must be heard by the person to whom the threat is directed, make the provision realistically redundant in the context of potential prosecution of online TFSV. Furthermore, in the UK, the key laws governing the communications offences—the Malicious Communications Act 1988<sup>56</sup> (MCA 1988) and the Communications Act 2003 (CA 2003)<sup>57</sup> are only partially suited for prosecution of modern day communication offences, including those involving TFSV. Primarily, the offences enshrined in the MCA 1988 and the CA 2003 focus on the misuse of a public network rather than the nature of the act committed or the effect it has on the recipient/victim. Furthermore, a very high threshold for both offences combined with the need to meet the public interest threshold for the prosecution make them unlikely avenues of redress in cases involving online TFSV. For instance, the threshold for satisfying a Communications Act offence under § 127, requires that the communication be “grossly offensive”—a threshold which is difficult to satisfy, and which has been the subject of criticism as a result.<sup>58</sup> This evidential threshold, even where satisfied, does not mean that there will be a prosecution—the public interest test also must be satisfied separately. Together, these thresholds mean that even though a criminal offence exists, it is not necessarily frequently utilized.

<sup>54</sup>For a detailed analysis of these categories of offences and their limited applicability to online abuse, including TFSV, see KIM BARKER & OLGA JURASZ, *supra* note 2, pp47–65.

<sup>55</sup>See Kim Barker & Olga Jurasz, *supra* note 17, at 79–100; see also Kim Barker and Olga Jurasz, *supra* note 52. KIM BARKER & OLGA JURASZ, *supra* note 2. See also Kim Barker & Olga Jurasz, *Online Misogyny as a Hate Crime: #TimesUp*, in MISOGYNY AS HATE CRIME (Irene Zempi & Jo Smith eds., 2021).

<sup>56</sup>Malicious Communications Act 1988, §1 (UK).

<sup>57</sup>Communications Act 2003, § 127 (UK).

<sup>58</sup>See Marit Majj, *Ending Cyberdiscrimination and Online Hate*, COUNCIL OF EUROPE (December 13, 2016), =<https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=23234>.

## II. Is the Criminal Justice System Fit for Dealing with OTFSV Cases?

Aside from the necessary legislative reform, broader questions arise about the capacity and suitability of the criminal justice system to deal with cases involving OTFSV. As the example of England & Wales shows, whilst there exists an overall commitment of the justice system to tackle cybercrime<sup>59</sup>—which, in theory, should include its gendered forms, such as OTFSV—in practice it is rather selective as to which cybercrimes are indeed tackled, largely to the exclusion of online forms of sexual violence, particularly those which are not image-based. For instance, the CPS Guidance on Social Media VAWG Offences states that “communications that contain images or videos of women with very serious injuries, or of women being raped, or of women being subjected to sadistic acts of violence, accompanied by text that suggests that such assaults/rape/acts are acceptable or desirable may well, depending on the context and circumstances, be considered grossly offensive.”<sup>60</sup> As such, whilst the Guidance acknowledges the possible gross offensiveness—and, what follows, harmfulness—of text-based dimensions of OTFSV, it sees it as merely accompanying feature of IBSA rather than a stand-alone type of OTFSV which may warrant prosecution. Furthermore, the test for public interest in prosecuting social media offences, which may include OTFSV, is relatively high and, following CPS Guidelines, it is likely to be met relatively rarely.<sup>61</sup>

Added to this is another complexity, the question of attitudes of the police and other actors in the justice system towards policing and accountability for acts of OTFSV. The misperceptions of the harmfulness of online abuse, especially where it takes sexual and/or gender-based forms, continue to permeate the justice system. Often seen as not ‘really’ violent—in the sense that offline acts of violence, such as knife crime or offline sexual offences, are—reports of online sexual abuse are often seen as a stretch on the limited police resources, even by the police chiefs.<sup>62</sup> The issue of

<sup>59</sup>Cybercrime is stated to be one of the UK National Crime Agency’s strategic priorities. See *Leading the UK’s Fight to Cut Serious and Organised Crime. Annual Plan 2020-2021*, NATIONAL CRIME AGENCY (Apr. 2020), <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/439-national-crime-agency-annual-plan-2020-2021-1/file>; see also Jamie Saunders, *Tackling Cybercrime – the UK Response*, 2 J. CYBER POL’Y, 4 (2017).

<sup>60</sup>*Social Media - Guidelines on Prosecuting Cases Involving Communications Sent Via Social Media*, THE CROWN PROSECUTION SERVICE (Aug. 21, 2018), <https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media>.

<sup>61</sup>See *Public Interest Stage of the Code for Prosecutors*, THE CROWN PROSECUTION SERVICE (Aug. 21, 2018), <https://www.cps.gov.uk/legal-guidance/social-media-guidelines-prosecuting-cases-involving-communications-sent-social-media>.

<sup>62</sup>“30. Prosecutors must be satisfied that a prosecution is required in the public interest and, where Article 10 is engaged, this means on the facts and merits of the particular case that it has convincingly been established that a prosecution is necessary and proportionate. Particular care must be taken where a criminal sanction is contemplated for the way in which a person has expressed themselves on social media.

31. Prosecutors therefore should, where relevant, have particular regard to:

a. The likelihood of re-offending. The spectrum ranges from a suspect making a one-off remark to a suspect engaged in a sustained campaign against a victim;

b. The suspect’s age or maturity. This may be highly relevant where a young or immature person has not fully appreciated what they wrote;

c. The circumstances of and the harm caused to the victim, including whether they were serving the public, whether this was part of a coordinated attack (“virtual mobbing”), whether they were targeted because they reported a separate criminal offence, whether they were contacted by a person convicted of a crime against them, their friends or family;

d. Whether the suspect has expressed genuine remorse;

e. Whether swift and effective action has been taken by the suspect and/or others for example, service providers, to remove the communication in question or otherwise block access to it;

f. Whether the communication was or was not intended for a wide audience, or whether that was an obvious consequence of sending the communication; particularly where the intended audience did not include the victim or target of the communication in question.

g. Whether the offence constitutes a hate crime (which may mean Article 10 is not engaged, but may also be a factor tending in favour of a prosecution in the public interest).”

<sup>62</sup>See Ben Quinn, *Met Police Chief Backs Call to Focus on Violent Crime Not Misogyny*, THE GUARDIAN (Nov. 2, 2018), <https://www.theguardian.com/uk-news/2018/nov/02/metropolitan-police-chief-cressida-dick-backs-call-focus-violent-crime-misogyny>.

resources is a valid one, albeit one that needs addressing through meaningful reform rather than being used as an excuse not to tackle online criminality.<sup>63</sup> The volume of various forms of online violence, including OTFSV, frequently paired with the anonymity of the perpetrators and the lack of appropriate and efficient reporting mechanisms pose a barrier to the effective processing of such cases. It is therefore difficult to envisage meaningful change with regard to OTFSV given the overwhelmingly negative attitude towards regulating and establishing accountability for these forms of violence on the one hand, and the practical barriers on the other.

Lastly, there remain significant questions over whether a meaningful criminal law reform addressing OTFSV is even possible. It is unlikely that new criminal laws—however modern and adequate—will be capable of addressing the underpinning causes of OTFSV, including patriarchy, structural gender-based violence, pervasive gender stereotyping, and gender-based inequality which permeates the societal structures. Feminist critique of criminal law has long highlighted the gender-bias of the criminal law and the justice system which ignores experiences of women and fails to conceptualize, prosecute, punish and redress harms suffered by women—especially those arising in relation to sexual offences.<sup>64</sup> Victim blaming, stereotypes surrounding gender roles, and trivialization of experiences of the victims of sexual violence are likely to be reproduced at trials of cases involving OTFSV due to the deeply entrenched biases of the justice system and actors involved in handling as well as adjudicating such cases. This, in turn raises doubts as to whether harms suffered by the victim of OTFSV would be legally recognized and redressed.

### III. Is Internet Law Fit to Respond?

Beyond questions surrounding the suitability of the criminal justice system to respond to deal with cases of OTFSV, there is the caveat that a substantial portion of the discussion inevitably must also fall within the sphere of online regulation and platform regulation more specifically. Historically, where regulation has been part of the legislative agenda, the emphasis has fallen on attempting to ensure that the internet remains workable,<sup>65</sup> but also protects the platform and website operators from burdensome responsibilities.<sup>66</sup> In so doing, the legendary e-Commerce Directive<sup>67</sup> is one of the first regional attempts to offer some element of regulation to internet platforms. It does not however actually regulate content—the content is something which is addressed through the introduction of the liability shield provisions<sup>68</sup> which have operated to ensure that platform operators are not responsible for the content that is posted and shared on their platforms. Criticisms of

<sup>63</sup>For instance, the case of Caroline Criado-Perez, a feminist campaigner who receives thousands of violent and sexually explicit and abusive tweets, demonstrates the multiple shortcomings of the police in handling reports of such abuse. See Caroline Criado-Perez, *Have the Police Failed to Record the Twitter Threats Against Me?*, NEW STATESMAN (Sept. 5, 2013), <https://www.newstatesman.com/voices/2013/09/have-police-failed-record-twitter-threats-against-me>. See also Caroline Criado-Perez, *Caroline Criado-Perez's Speech on Cyber-harassment at the Women's Aid Conference*, NEW STATESMAN (Sept. 4, 2013), <https://www.newstatesman.com/internet/2013/09/caroline-criado-perezs-speech-cyber-harassment-womens-aid-conference>.

<sup>64</sup>See e.g., DONALD NICOLSON & LOIS BIBBINGS, *FEMINIST PERSPECTIVES ON CRIMINAL LAW* (2000); see also Prabha Kotiswaran, *Feminist Approaches to Criminal Law*, in *THE OXFORD HANDBOOK OF CRIMINAL LAW* (Markus D. Dubber & Tatjana Hörnle eds., 2014); see also Sharon Cowan, *Sense and Sensibilities? A Feminist Critique of Legal Interventions Against Sexual Violence*, 23 *EDINBURGH L. REV.* 22-51 (2019); see also NGAIRE NAFFINE, *CRIMINAL LAW AND THE MAN PROBLEM* (2019); see also JOANNE CONAGHAN, *LAW AND GENDER* (2013); Kim Barker & Olga Jurasz, *supra* note 2, at 8–10.

<sup>65</sup>Or, as Savin suggests, the Internet requires regulation which is different – and beyond – the norms of legal governance. See ANDREJ SAVIN, *EU INTERNET LAW* 10 (2017).

<sup>66</sup>See TARLETON GILLESPIE, *CUSTODIANS OF THE INTERNET* 79 (2018).

<sup>67</sup>Directive 2000/31, of the European Parliament and of the Council of June 8, 2000, on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce,') 2000 O.J. (L178) 1 (EC) [hereinafter e-Commerce Directive 2000].

<sup>68</sup>*Id.* at arts 12–15.

these provisions have abounded in recent years,<sup>69</sup> not least from the platforms themselves who have sought to refrain from becoming involved in so-called editorial roles and therefore have been able to remain within the protections of the liability shields.

That said, given the rise of OTFSV, and other online harms, there has been a growing appetite for addressing online content through legal regulation. This has resulted in the Online Harms White Paper<sup>70</sup> in the UK for example, which is intended to lead to legislation introducing a statutory duty of care.<sup>71</sup> This duty, which still requires some clarification in terms of its proposed operation, has been watered down from initial suggestions that executives of online platforms would be criminally prosecutable for non-compliance with the Online Harm regime.<sup>72</sup> Other examples of initiatives designed to address regulation include the German Network Enforcement Act<sup>73</sup> which focuses on hate speech and hateful content online and takedown penalties for online platforms which are non-compliant within specific timescales. These are not the only examples—Austria,<sup>74</sup> and France<sup>75</sup> have also introduced proposed legislation to address elements of the internet regulation. While these legislative developments are not specifically designed to address the OTFSV phenomenon, they do represent a shift in attitudes towards internet regulation.

That said, the difficulty in all of these remains one of enforcement. Moreover, the proposed Digital Services Act, tabled by the European Parliament in December 2020<sup>76</sup> indicates that there will be a greater obligation imposed on platform operators to ensure that online content is not illegal. This changes significantly the position operators have enjoyed under the current eCommerce Directive and its regime. There are nevertheless stark signals that this will change, and there is appetite from platform operators<sup>77</sup> for this to be the case. What remains unseen is how these various provisions are supposed to be enforced and utilized. In all situations, especially for those in continental Europe, there remains the question of how varying national regimes fit into the framework proposed by the DSA.

If platforms and their operators are subjected to greater responsibilities and have to now take an active role in content control, as has been suggested through the DSA proposal, this is likely to cause potential problems for users. Where liability is to be imposed on the platform, this could lead to over-zealous platform actions to protect their own interests. They are after all, commercial and profit-driven entities who will be seeking to mitigate their potential liabilities. More importantly with no specific thought given to how the criminal law may be dealing with OTFSV, there seems to be little joined-up thinking being considered to ensure that OTFSV is a key consideration in changes to the legal frameworks address internet regulation. Similarly, no matter how well thought out proposed changes to legal regimes are, it is incredibly unlikely that any internet

<sup>69</sup>See Aleksandra Kuczerawy, *Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative*, 31 COMPUT. L. AND SEC. REV. 1, 46–56 (2015). See also Aleksandra Kuczerawy, *The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression*, 8 JIPITEC 226, 227 (2017).

<sup>70</sup>HM GOVERNMENT, ONLINE HARMS WHITE PAPER: FULL GOVERNMENT RESPONSE TO THE CONSULTATION, 2020, [Cmd.] 354 (UK).

<sup>71</sup>*Id.* at Box 4.

<sup>72</sup>See Charles Hymas, *Social Media Bosses to Escape Sanctions as Govt Accused of Watering Down Duty of Care Laws*, THE TELEGRAPH (Dec. 11, 2020), <https://www.telegraph.co.uk/news/2020/12/11/social-media-bosses-escape-sanctions-govt-accused-watering-duty/>.

<sup>73</sup>Netzwerkdurchsetzungsgesetz [NetzDG] [Network Enforcement Act], Oct. 1, 2017, BUNDESGESETZBLATT [BGBl.] (Ger.).

<sup>74</sup>See KOMMUNIKATIONSPLATTFORMEN-GESETZ [KOPL-G] [COMMUNICATION PLATFORMS ACT 2020] BUNDESGESETZBLATT [BGBl.] No. 151/ 2020, as amended, <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011415>.

<sup>75</sup>Loi 1785 du 13 Mai 2020 Project de loi Avia [Law 1785 of May 13, 2020 on Aiming to Fight Against Hatred on the Internet ('Avia' Bill)].

<sup>76</sup>See *Regulation of the European Parliament and of the Council on a Single Market For Digital Services*, *supra* note 16.

<sup>77</sup>See Twitter, Mozilla, Automattic & Vimeo, *Crossroads for the Open Internet*, TWITTER PUBLIC POLICY (Dec. 9, 2020), [https://blog.twitter.com/en\\_us/topics/company/2020/crossroads-for-the-open-internet.html](https://blog.twitter.com/en_us/topics/company/2020/crossroads-for-the-open-internet.html).

law will be able to tackle the underlying causes of OTFSV. In sum, while internet regulation may prove capable of responding, the issue remains as to how effective that response is likely to be.

The recent proposals for reform in the context of online harms in UK do not raise much hope for a meaningful and gender-sensitive capturing of such harms.<sup>78</sup> Disappointingly, although not entirely unexpectedly, the emphasis of the reform seems to fall from considering harms associated with TBSA leaving, once again, little hope for paving the way to justice, however imperfect, for the victims of OTFSV.

#### D. International Responses to the Phenomenon of Digital Sexual Violence

The rise in online violence against women (OVAW), including OTFSV, has prompted responses from key actors at international and regional levels, such as the United Nations and the Council of Europe.<sup>79</sup> As there is no supranational and universally applicable criminal law regime regulating OVAW nor OTFSV, these responses have been largely framed within the scope of human rights obligations of states. Nonetheless, within this context and given the remits of the aforementioned bodies, the need for implementation of adequate responses to OTFSV, including criminal law measures, has been highlighted.

In 2018, the UN Special Rapporteur on Violence Against Women, its Causes and Consequences (UNSRVAW) recognized the diverse nature of online violence against women, including its sexualized forms:

[O]nline and ICT-facilitated acts of gender-based violence against women and girls include threats of such acts that result, or are likely to result, in psychological, physical, sexual or economic harm or suffering to women. (. . .) ICT may be used directly as a tool for making digital threats and inciting gender-based violence, including threats of physical and/or sexual violence, rape, killing, unwanted and harassing online communications, or even the encouragement of others to harm women physically.<sup>80</sup>

Furthermore, the UNSRVAW highlighted multiple shortcomings in relation to states' general inaction with regard to addressing online violence against women—especially concerning access to justice and a right to remedy<sup>81</sup>—and recommended that states should comprehensively criminalize OVAW.<sup>82</sup>

At the European level, the recent focus has largely fallen on tackling OVAW, including its sexualized forms, through tackling gender stereotypes and sexism rather than suggesting any avenues of harmonization of criminal laws concerning OVAW. To that end, the Council of Europe (CoE)

<sup>78</sup>For a critique of these proposals, see Kim Barker & Olga Jurasz, *Online Harms White Paper Consultation Response*, THE OPEN UNIVERSITY (2019), <http://oro.open.ac.uk/69840/>. See also Kim Barker & Olga Jurasz, *Online harms and Caroline's Law – What's the Direction for the Law Reform?*, SCRIPTED (Apr. 13, 2020), <https://script-ed.org/blog/online-harms-and-carolines-law/>; Kim Barker & Olga Jurasz, *Reform of the Communications Offences - Consultation Response to the Law Commission*, THE OPEN UNIVERSITY (December 2020) [on file with authors], <http://oro.open.ac.uk/75091/>.

<sup>79</sup>United Nations Human Rights Council, *Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective*, U.N. Doc. A/HRC/38/47 (June 18, 2018); *Council of Europe Gender Equality Strategy 2018-2023*, CoE (Jun. 2018), <https://rm.coe.int/prems-093618-gbr-gender-equality-strategy-2023-web-a5/16808b47e1>. For detailed analysis concerning OVAW in Europe, see Kim Barker & Olga Jurasz, *supra* note 4.

<sup>80</sup>United Nations Human Rights Council, *Report of the Special Rapporteur on Violence Against Women, Its Causes and Consequences on Online Violence Against Women and Girls from a Human Rights Perspective*, U.N. Doc. A/HRC/38/47, at paras. 27 & 31 (June 18, 2018).

<sup>81</sup>*Id.* at paras. 81–83, 85.

<sup>82</sup>*Id.* at paras. 100–02.

Gender Equality Strategy stresses the need to tackle violence against women—both online and offline—through combatting gender stereotypes and sexism—including sexist hate speech and violent and sexualized threats online, especially on social media platforms.<sup>83</sup> Furthermore, the Parliamentary Assembly of the CoE (PACE) has called for ending sexual violence and harassment of women in public spaces<sup>84</sup>—a goal that is also embedded in the 2019 CoE Recommendation on Preventing and Combating Sexism<sup>85</sup>—the first ever international legal instrument to combat sexism.

However, the CoE Convention on preventing and combating violence against women and domestic violence 2011 (the Istanbul Convention), whilst not explicitly referring to OVAW, is clearer and more focused on state parties' obligations in the realm of criminalization of various forms of violence against women. These include psychological violence, Article 33, stalking, Article 34, sexual violence, Article 36, sexual harassment, Article 40—for example, forms of violence against women which frequently take place online and which can take sexualized forms. That said, given the backlash towards the Istanbul Convention in some of the Central and Eastern European states and the lack of EU accession to the treaty, the future of states fulfilling their obligations in relation to combatting online VAW is uncertain. Equally, Ursula von der Leyen's commitment to list violence against women as one of the 'Eurocrimes' in the EU Treaty,<sup>86</sup> whilst bearing some promise for uniformity of approaches and universal approach towards holding perpetrators of OVAW to account is, practically speaking, unlikely to include sexualized forms of OVAW.

Despite the overwhelming fragmentation of European responses towards tackling OVAW,<sup>87</sup> some degree of harmonization—albeit more in relation to policy than law—is theoretically possible to achieve amongst the states that ratified the Istanbul Convention. The four pillars (4 'Ps') of the Convention provide a useful framework of assessment of progress and gaps in the realization of state obligations under the Convention. As one of the pillars refers to prosecution, it is in principle possible for the monitoring body GREVIO to provide guidance to state parties on how the criminal law ought to address OTFSV, and OVAW more broadly. It is hoped that the forthcoming Recommendation of GREVIO on online and technologically facilitated violence against women and girls will be the first step in this direction.

## E. Conclusions: Towards a Comprehensive Regulatory Response?

The phenomenon of OTFSV poses, as this article has indicated, a number of challenges for the criminal law, but also for the legal system more broadly. OTFSV remains a conceptual struggle for the legal framework—both in distinguishing between the harms caused, and the forms of behavior that give rise to those harms. Beyond this, there is a persistent, and clear lack of willingness to take responsibility from a number of different elements of the justice system. The mixed messaging surrounding the distinction between online & offline compounds the challenges surrounding OTFSV. Such confused messaging is also prevalent in the different approaches being mooted by the EU in its Digital Safety Act, and European states who are introducing different approaches

<sup>83</sup>Council of Europe Gender Equality Strategy 2018-2023, CoE (Jun. 2018), <https://rm.coe.int/prems-093618-gbr-gender-equality-strategy-2023-web-a5/16808b47e1>.

<sup>84</sup>PACE, Resolution 2177 on putting an end to sexual violence and harassment of women in public space, June 29, 2017. It is worth noting that the document does not distinguish between online and offline space. For purposes of this article, the authors understand online spaces as public spaces.

<sup>85</sup>Recommendation on preventing and combating sexism, CoE (Mar. 27, 2019), <https://rm.coe.int/prems-055519-gbr-2573-cmrec-2019-1-web-a5/168093e08c>.

<sup>86</sup>Ursula Von der Leyen, *A Union that strives for more. My agenda for Europe. Political guidelines for the next European Commission 2019-2024*, [https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission\\_en\\_0.pdf](https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf), (last visited May 28, 2021).

<sup>87</sup>For a detailed analysis of the European responses to OVAW, see Kim Barker & Olga Jurasz, *supra* note 4.

to internet regulation, and internet content regulation. This reiterates the continual ‘passing’ of responsibility from one branch of the law to another, without any holistic thinking being adopted to address the issues. In many respects, both criminal law, and internet regulation should come together to tackle OTFSV, and learn from other movements, such as #MeToo, to bring the broader sexual harassment undercurrents to the fore, and facilitate a workable response.

Ultimately, in order to meaningfully address OTFSV, the criminal law must capture this form of conduct so as to allow effective mechanisms of redress to be created. Further inaction will only contribute to a continuum of sexual violence and further violence against women.