KnowEx Social Sciences Journal
Vol.2, No.1, 59-72, 2021, ISSN 2705-9901 (Online)

DOI: https://doi.org/10.17501/27059901.2021.2105

EUROPEAN 'RIGHT TO BE FORGOTTEN' AS A REMEDY FOR IMAGE-BASED SEXUAL ABUSE: A CRITICAL REVIEW

Nguyen TNA*

MA Human Rights and Multi-level Government, University of Padova, Italy

Abstract: Image-based sexual abuse, defined as the non-consensual creation or dissemination of private sexual images, has been proved to be a form of sexual violence against women. Despite the borderless impacts of image-based sexual abuse due to its online nature, very little scholarly attention has been given to the legal remedies that victims can take in a more regional context. This article advocates for a new joined-up approach that supports victims of image-based sexual abuse to reclaim control through the right to be forgotten under European data protection law. Under this right, the victims as data subjects can request the data controllers – service providers hosting abuse materials – to erase their non-consensual private sexual images from the platforms. Case study method was conducted with Google, Facebook and Telegram to evaluate the effectiveness of this approach, focusing on three main critiques: platform policies, reporting options, and removal practice in response to image-based sexual abuse. Based on the analyses of these digital platforms' policies and practices, the research identifies five challenges and limitations: (1) limited extraterritorial application of domestic law while dealing with transnational abuse; (2) ambiguous language about how to remove data; (3) absence of standardised terms to define and address all forms of image-based sexual abuse; (4) lack of liability fulfilments from digital platforms; and (5) lack of multi-stakeholder cooperation addressing the abuse. The research concludes that the right to be forgotten is a promising remedy to protect victims of image-based sexual abuse in this digital era, but it needs a multi-stakeholder approach to be able to keep up with transnational violence like image-based sexual abuse.

Keywords: image-based sexual abuse, right to be forgotten, gender-based cyber violence, data protection law, technology-facilitated sexual violence

Introduction

The technological advancements together with the diffusion of digital platforms, have created image-based sexual abuse (IBSA), a new pernicious form of sexual violence against women (SVAW). IBSA is understood as the non-consensual creation or sharing of private sexual images, including the threats to distribute them (McGlynn *et al*., 2017, 2020; Powell *et al*., 2019). The effects of IBSA can vary from egregious psychological to physical impacts, inhibiting sexual expression through victim-blaming and violation of victims' rights to privacy (Henry & Powell, 2016; McGlynn *et al*., 2019, 2020). Moreover, due to the technological nature and online contexts, the impacts of IBSA are not

Corresponding author's email: thingocanh.nguyen@studenti.unipd.it
ORCID iD: https://orcid.org/0000-0002-2401-0591

only the results of image sharing but also the subsequent harassment, shaming, and abuse due to the wide dissemination of abuse materials online (McGlynn *et al*., 2019, 2020).

Above all, as IBSA is not defined as sexual abuse in many legislations, victims may not be given anonymity throughout the trial (McGlynn *et al*., 2019). Even though legal redress and justice for victims of IBSA have been researched (e.g., Henry *et al*., 2018; Rackley *et al*., 2021; Stevenson-McCabe & Chisala-Tempelhoff, 2021), little scholarly attention has been given to the remedies in a more regional and global context. In addition, Henry *et al*. (2020, p. 1843) point out that criminal and civil laws are the most common legal approach in response to IBSA, but they have to face many obstacles such as "inconsistent laws, a lack of police resources, evidentiary limitations, jurisdictional boundaries, and victim blaming or harm minimisation attitudes." They further argue that victims need other measures in response to the harms of IBSA besides criminal and civil remedies. McGlynn *et al*. (2019) also highlight that a support system for victims to reclaim control is essential, including the way to remove their non-consensual private sexual images from online sources. It is, therefore, necessary for further research about better protection for IBSA victims, taking the features of borderless online contexts into consideration.

This article addresses these research gaps by examining a new approach – data protection law – to protect victims of IBSA in a post-violence context. In general, although social media may not directly cause harm, they do contribute to the widespread of IBSA (Laville, 2016). In this context, the General Data Protection Regulation (GDPR) became enforceable in 2018, addressing personal data protection in the European Union (EU) and the European Economic Area (EEA) and the transfer of personal data outside these areas. The GDPR has become a helpful tool in combating IBSA because it directly impacts the dissemination of personal data and private sexual images. Among the data protection rights codified in the GDPR, the right to be forgotten (RTBF) or "right to erasure" has attracted significant public attention. The RTBF names the data subject's right to ask data controllers such as search engines or digital platforms to remove specific data related to them. The hypothesis is the find how the RTBF under European data protection law can be applied to erase IBSA materials from digital platforms hosting harmful content. And more importantly, what are the obstacles to implementing this new approach in response to IBSA? Images of minors are disseminated without consent as well, but this aspect falls into the category of 'child abuse material' and is addressed by child pornography laws. As the issue has been extensively analysed, this research focuses only on adult women (18 years old or higher) as victims of IBSA.

The author conducted a desk review based on legal sources and literature on data protection law, the RTBF, and image-based sexual abuse to explore the potential of the RTBF as a remedy for IBSA. Based on this background, the case study method was chosen because of the need to explore this new joined-up approach "in depth and in its natural context" (Crowe *et al*., 2011, p. 1). The case study method generates an in-depth understanding of how digital platforms apply the RTBF within a real-life context, and its effectiveness in relation to IBSA. In particular, the article selected three of the most prominent platforms - Google (a search engine), Facebook (a social media), and Telegram (a messaging app). The research platforms have been selected based on their traffic, market dominance, capacity to host IBSA content and popularity as ranked by Alexa (Alexa Internet, n.d.) and Statista (Statista, 2021). The author identified these companies' privacy policies, terms of service, transparency reports, answers to FAQs, and official blogs as a basis to investigate the respective

platforms. Each document is analysed to determine whether they have specific IBSA policies or general policies that could apply to IBSA for either reporting, blocking, or erasing non-consensual content. Relevant media news, blogs, and journal articles on these platforms' actions to respond to IBSA content from various database are also analysed to evaluate the practices of the RTBF as a remedy for victims of IBSA in the most comprehensive way. The research looks at three critical factors: platform policies, reporting processes and removal practices.

It is also essential to recognise the limitations of this study. The article could only investigate publicly available policy documents. For this reason, the author was unable to review the unpublished standards that administrators follow behind closed doors, and information regarding private automated technologies that digital platforms might utilise. Next, by choosing the most popular companies to analyse, the research could not investigate small tech companies, pornography sites, nor could it explore the fringe or underground platforms such as those operating in the darknet where IBSA material is being posted. Lastly, the research could not directly examine the opinions of either victims or platform representatives in connection to data erasure policies or practices.

Right to be Forgotten under European Data Protection Law

The RTBF, as a result of the 2014 Court of Justice of the European Union (CJEU)'s judgement in Google Spain, set a precedent for the "right of erasure" provision contained in the GDPR. The GDPR enacted a "Right to erasure (Right to be forgotten)" in Article 17, stating that "[t]he data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have an obligation to erase personal data without undue delay." It also states that personal data must be erased right away if they are no longer required for their original processing purpose, the data subject has withdrawn his consent, and there is no other legal ground for processing, the data subject has objected, and there are no overriding legitimate grounds for processing or erasure is required to fulfil a statutory obligation under EU law. Besides, if the processing was illegal, to begin with, the data has to be removed.

As a result, the controller is subject to statutory erasing requirements and, at the same time, must comply with the data subject's right to erasure pursuant to Article 17 GDPR. However, the regulation makes no mention of how data shall be deleted in certain situations. It is adequate if the data media has been physically destroyed or if the data has been permanently overwritten with specialised software (Intersoft Consulting, n.d.). Furthermore, according to Article 17(2) of the GDPR, if the controller has made the personal data public and one of the aforementioned reasons for erasure exists, the controller has to "take reasonable steps" to notify about the erasure of "any links to, or copy or replication of, those personal data" to controllers processing data.

However, the RTBF is not absolute and, thus, is restricted in some situations, especially when it conflicts with the right to freedom of expression and information (EU General Data Protection Regulation, art 17(3)(a)). Other exceptions include when the processing that is subject to an erasure request is essential to comply with "legal obligations," for "archiving purposes in the public interest", scientific or historical research purposes, or statistical purposes, or for the "defence of legal claims" (EU General Data Protection Regulation, art 17(3)). The GDPR supports the CJEU's opinion that the data subject has the right to seek the removal of online content, "override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in

finding that information upon a search relating to the data subject's name" (*Google Spain and Google v. AEPD*, 2014).

Furthermore, the extraterritorial scope of the GDPR has resulted in major problems, primarily with the RTBF, as the CJEU has sought to determine the conditions under which demands to erase online material bound controllers based overseas with global effect (Fabbrini & Celeste, 2020). In 2019, the CJEU ruled on this issue in two cases involving Google and Facebook, paving the way for the implementation of EU law on a global scale (Fabbrini & Celeste, 2020). In particular, the CJEU held that there is no obligation under EU law for Google, and other search engine operators, to apply the European RTBF worldwide (*Google c. CNIL*, 2019). The Court also underlined that nothing precludes the Member States from allowing for worldwide dereferencing where the preservation of privacy and personal data exceeds the guarantee of other rights (Fabbrini & Celeste, 2020). Even though this ruling seems to narrow the effects of GDPR, the decision in *Glawischnig-Piesczek v. Facebook* (2019) balanced it when the CJEU suggested a worldwide impact as a preferred remedy, subject to international law compliance.

Right to be Forgotten as a Remedy for Image-Based Sexual Abuse

The ability to stay anonymously online has made it difficult to hold perpetrators accountable for what they did to others in the virtual world. The combination of secrecy without carrying any responsibilities has created an ideal breeding ground for IBSA. McGlynn *et al*. (2019) state that a support system for victims to reclaim control is essential, including a way to remove their non-consensual private sexual images from online sources. In light of this context, the RTBF is much-needed in providing a remedy for victims of IBSA for several reasons.

First, the RTBF further limits the harmful impacts of IBSA in real life, mainly due to online reputation damage. The RTBF makes a difference in unravelling this issue, thus becoming an essential answer to prevent career destruction or discriminatory practices based on something that is not even the fault of victims (Reicherts, 2014). When the IBSA materials are deleted from the online space, people who do internet searches will no longer be inundated with them. This will further help the victims keep their financial status stable and stabilise their lives faster after trespassing. Citron (2014) highlights that the ability to have content erased could be lifesaving for victims who fear that a brutal invasion of privacy could ruin their lives.

Second, the RTBF can protect and promote victims' privacy and autonomy. Undoubtedly, protecting these rights has become increasingly complex with the rise of the Internet and online search engines because of their global and unlimited reach. Ku & Lipton (2010) express an idea about a right to freedom not to speak as a critical aspect of autonomy. As the opposite of freedom of expression, "this freedom not to speak protects the right not to have information disclosed without consent or in a manner contrary to one's interests" (Ku & Lipton, 2010). The ability not to speak in virtual worlds might be as easy as refusing to have one's images displayed online without their consent. Unfortunately, this option is no longer available for most people. Even without our permission, photographs, videos, or other personal data may be disseminated online. As a result, the Internet has deprived us of both privacy and autonomy. It means that our options to keep something about ourselves personally, as well as our freedom not to speak, have gone. When private sexual images are disseminated without consent, the consequences may be disastrous for that person. Moreover, the

effects can be lethal since online harassment is more prone to cause significant mental anguish in the young (Citron, 2014). In this context, removing non-consensual private sexual images can become a way for victims to reclaim their control over their personal information by being able to choose not to disclose them to people they do not want to. Consequently, the RTBF not only returns the power to control to victims of IBSA but also promotes their privacy and autonomy online.

Last but not least, the RTBF can become a legal tool to protect victims from perpetrations and further give them the means to fight back against their abusers (Edwards, 2014). One of the main reasons for SVAW is the man's desire to control and subjugate women and make them vulnerable to further harm. In the online context, this is even worse when victims cannot escape from the abuse because of the straightforward nature of sharing pictures online. Further, contacting the website operators to ask for removing the abuse material is often complicated and sometimes takes a long time without proper guidelines. However, this is not the case anymore with the enforcement of the GDPR that is legally binding for data controllers hosting abuse materials on their platforms. The RTBF becomes a legal tool for victims to remove the main reason they have to suffer all these harmful impacts – their non-consensually distributed private sexual images. Victims finally have the ability to flee the perpetration by having the violent content deleted from the online world.

In practice, it appears that the RTBF did have a positive impact on the platforms' policies addressing IBSA. In particular, Google has to comply with the 2014 judgements of the CJEU and allow people who are residents of a European country to ask for the removal of "inadequate, irrelevant or excessive" data (*Google Spain and Google v. AEPD*, 2014). It soon influenced Google's policy when the search giant decided to publish a new policy about removing non-consensual intimate sexual images from its search results for all victims of IBSA in 2015. The approach allows data subjects or their representative to send removal requests to Google, asking for the removal of "non-consensual explicit or intimate personal images", "involuntary fake pornography", and "content about me on sites with exploitative removal practices" from its search results. However, it only considers the URLs connected to the search key of the data subject's name, which means the links can still show up in the search results with other keywords (Google, n.d.). If the request is refused, the data subject can ask for the removal of IBSA content under the RTBF in accordance with the EU data protection law if they are EU residents. But in this case, Google only removes the URLs within the EU borders following the CJEU's ruling in *Google v. CNIL*.

In the field of social media, Facebook proves its acknowledgement towards its colossal power to control people's data and how every decision it makes can affect people's lives. Since 2017, Facebook has continuously updated its policies, including data policies, terms of service, community standards, to address and respond to IBSA content. The platform does not allow people to share or threaten to share "sextortion" content, "revenge porn" or "non-consensual intimate images", and "upskirts" content. It bans the "non-consensual [sharing of] intimate images" according to three factors: the content is "non-commercial" or "produced in a private setting"; the individual depicted is naked, almost naked, engaging in a sexual act, or posing sexually; and there is a lack of consent indicated by "vengeful context" (such as captions, comments, page titles), independent sources, or allegations from victims or others. With upskirting content, Facebook bans the distribution of secretly taken non-commercial imagery of a person's commonly sexualised body parts or a person engaged in sexual activity (Facebook, 2021b). Moreover, reporting IBSA content on Facebook is simple and convenient

because the report option is attached to every post, comment, story, private message, or other content. The current policies give victims worldwide options to have a theoretical right similar to the RTBF, in which they can ask Facebook to take down their private sexual images distributed without consent. It also addresses more forms of IBSA than Google, namely revenge porn, sextortion, upskirting. If unsuccessful in asking for the removal of abuse content in this way, victims who are residents in the EU can ask for their RTBF under the GDPR by filling a special form on the website.

In the last case, Telegram has stated that it aims to provide a "truly free messenger, with a revolutionary privacy policy" (Telegram, n.d.-a). Keeping that mindset in its heart of service, Telegram only processes any removal requests concerning "illegal pornographic content" sharing on "publicly viewable" channels or bots of Telegram (Telegram, n.d.-b). Data subjects can only claim their RTBF or their right to "delete […] personal data" under GDPR, but it only applies to data that they have access to (Telegram, 2021). These include their accounts on Telegram (messages, media, contacts and every other piece of data they store in the Telegram cloud), their messages in secret chats, cloud chats, groups and channels, their messages and their partner's messages in one-on-one chats (Telegram, 2021). For other personal data shared "privately" between other users, including non-consensual private information, victims cannot ask Telegram for their RTBF.

Finally, it is worth noticing that since only the most severe infractions of data protection would become subjects to erasure according to the law, the RTBF is unlikely to address all privacy and autonomy concerns in the online world. Even yet, if the information is valid and relevant, privacy infractions will not necessarily fulfil the threshold for deletion under the legislation. This issue will be further discussed in the next section of the paper. Still, the new GDPR-compliant RTBF does enable redress for those who have had their private sexual images and, in some instances, personal information disseminated without consent (Cook, 2015).

The Challenges and Limitations in Protecting Victims of Image-Based Sexual Abuse

This section seeks to define the challenges and limitations of the RTBF pursuant to the GDPR in tackling IBSA and fulfilling its role as a remedy for victims. Given the transnational nature of IBSA, there is an urgent need for international laws and regulations. As such, differences in the scope and extraterritorial application of domestic data protection laws between countries and regions make it difficult for victims to ask for protection and support when a crime is committed in another country. Further, asking for the erasure of abuse materials is a transnational issue but largely dependent on domestic legal jurisdictions. Significantly, the role of the RTBF in protecting victims of IBSA and the non-consensual sharing of private sexual images forms a subset of the broader debate around the need for technology providers to "do more" in addressing online harms.

The limited extraterritorial scope of the GDPR in tackling transnational violence

Unlike SVAW happening in the offline context, IBSA transcends any national border, and thus, it requires transnational remedy. This also means that, except for countries where the Internet is not available, almost anyone could anonymously upload non-consensual sexual images, and almost anyone could have access to these abuse materials. As a result, the current limited territorial scope of the RTBF under GDPR is a part of why it fails to address actual abuse in cyberspace. It indicates that, in addition to consistent data protection standards inside the region, EU data protection rights or the

RTBF should have extraterritorial implications beyond its border (Fabbrini & Celeste, 2020). However, the extraterritorial implementation of EU data protection legislation raises several issues, such as conflict with the international comity obligations or the need to respect the diversity of legal systems (Fabbrini & Celeste, 2020). The European Data Protection Board said it could not comment on data protection in the IBSA scenario because it has "yet to issue guidance on this topic specifically," but also noted that it is "currently developing further guidance on data subject rights" (Cater, 2021).

Given these concerns, the recent CJEU decisions regarding Google and Facebook might be considered as a rational approach attempting to bridge the gap "between the Scylla of data protection imperialism and the Charybdis of digital sovereignty" (Fabbrini & Celeste, 2020). Indeed, arguments between these conflicting movements will only worsen. Whereas the 'imperialist' attitude of EU data protection law has been criticised (Prasad, 2019; Svantesson, 2015), other recent developments, such as moves by governments worldwide to assert sovereign control over data, reveal the possibility of fragmentation of the online realm. Diverse arguments to "digital sovereignty" are growing worldwide, possibly leading to a steady loss of fundamental rights online (Fabbrini & Celeste, 2020). Developing international legal frameworks appears to be the essential way to sustain digital human rights for everyone, including the right to privacy, data protection, or further the RTBF. And IBSA victims are the ones who need a global application beyond the borders of these rights the most in this scenario.

Lack of "erasure" definition in the cyber context

Another limitation comes from the lack of a clear definition for the terms "erasure" and "erase", used to describe the RTBF in Article 17 of the GDPR. From a technical point of view, the term "erasure" refers to the action of wiping out the data completely so that it cannot be recovered anymore. By contrast, "delete" means removing and forgetting the data inside the system's storage. The 'deleted' file is recoverable, and it will only disappear when it is overwritten with new information (Gutmann & Warner, 2019). Since the GDPR does not give any instruction on how the data should be erased, it leaves the ground for digital platforms to decide by themselves.

Google refers to the action of asking for the RTBF as "remove", and in case the URLs are removed, they are still accessible if users search with different keywords. Telegram states in their privacy policy that data subjects have the right to "delete" their personal data, and the app will process "take down" requests from third parties concerning illegal content. It does say that for personal data from the data subject's own account, all "will be flushed from our system" and that such action "cannot be undone" (Telegram, n.d.-a). In the case of Facebook, it says that the data subjects have the right to "erase" their data under the GDPR (Facebook, 2020), but the platform does not provide any additional information. It is still unclear whether the data actually disappeared or is just 'forgotten' somewhere, and thus, it is recoverable whenever the social media platform changes its mind. Indeed, Facebook did recover content that was erased because of adult nudity and sexual activity reason, as stated in the Transparency Report (Facebook, 2021a).

It is clear that the gap in how data controllers handle illegal data in their systems is the result of lacking comprehensive definition explaining how data should be erased from the law. Without a complete view of the data structure, it would be highly challenging to comprehend the depth of a data protection violation properly and how many victims it may have affected.

Vague and ambiguous phrases addressing IBSA

Terminology shapes legal redress arguments and thus has an essential communicative function. However, there is a variety of different adopted terms by each platform when it comes to IBSA (see more information in Appendix), in which not all forms of IBSA are addressed and taken seriously. Such inconsistency in how IBSA is mentioned can make it challenging for victims to deal with the digital platforms. Google, for example, has refused to remove IBSA content, including rape videos, because the search engine claims they look like "commercial porn" or "regret porn" (Goldberg, 2019).

The problem is specifically extended to the case of 'fakeporn'. Currently there are no official guidelines about its relation to personal data and whether it is subject to be erased under GDPR, leaving the matters to the digital platforms to decide again. In particular, Google allows its users to ask for deletion of "involuntary fake pornography" if the content "identifiably" portrays victims (Google Search Help, 2021). However, 'identifiably' is a broad word, and the only authority who would decide if the content were 'identifiably' enough to be removed is Google, not the victims. Facebook's policy, on the other hand, appears to target modified false news rather than IBSA materials. The social media platform only takes down "edited or synthesised" content resulted by AI or machine learning that can "mislead" people believe that the video subjects said words they did not say (Facebook, 2021c). This makes it indeterminate whether pictures, videos with no sound (for example, people's faces in porn films without sound are replaced with victims' faces) or products of low-tech, non-AI alteration (e.g., 'shallowfakes'[1]) would be included. In contrast, Telegram does not mention anything related to 'fake' content in its policies and guidelines. So only the messaging app can answer the question of whether fakeporn materials are considered "illegal pornographic" or promoting violent content according to its terms of service. Nevertheless, the site continues to host these contents, including bots that auto-creates deepfake images and both groups and channels sharing them (Semenzin & Bainotti, 2020; Vincent, 2020).

After all, the absence of standardised terms to define and address all forms of IBSA can make it difficult for service providers to target the abuse content and focus on the concerns of victims. Consequently, it can lead to the limit in practising the RTBF for victims, as the platforms may deny the removal requests because the content is not subject to be deleted according to the law or their policies. Further, it may lead to the minimisation of the victims' experiences by those in power, like what women used to face in history (Coombs, 2021).

Liability of the service providers

Given that digital platforms are the main factors that create the space for any abuse to happen in the first place, it is crucial to analyse their liability in this situation. There are various issues surrounding the practices of service providers in fulfilling their liability. First, it is demonstrated that even though digital platforms have to work under the data protection law, the outcomes still depend on the data controllers whether they fulfil their liability or not. Except for unlawful materials, internet intermediaries hosting or distributing content are typically not liable for what their users share. Even so, they are still the ones who decide what is considered illegal in most situations. In fact, digital

[1] Shallowfake is a method of manipulating media content utilising simple video editing software to alter existing media content, and thus, creating fake news to spread false contents (Johnson, 2019).

platforms not only hold “unprecedented power” (Suzor, 2019, p. 8) over what users view and disseminate but also have “broad discretion to create and enforce their rules in almost any way they see fit” (Suzor, 2019, p. 106). This is problematic as the decision-making process of seemingly "private" service providers could have severe consequences for individuals as well as wide-ranging ramifications for public spheres in general (Henry & Witt, 2021, p. 753).

Second, there is often a transparency gap between the policies in paper and the actual content review and removal practice. It is also unclear to precisely determine who reviews the reported content and who decides the final judgment (such as a content reviewer or a group of them) without access to the internal network (Witt *et al*., 2019). As a result, no one can evaluate how effective or ineffective a tech company has been in reacting to erasure requests from data subjects who are victims of IBSA and further preventing the abuse on their platforms.

Some technological businesses have experienced public attention for their opaque content filtering methods (Hopkins, 2017), leading to a transparency improvement on these corporations in some cases like Facebook or Google. However, their reports are still vague and do not break down the prevalence of IBSA materials nor the actions they took to take down such content, and how the content is actually removed from their systems (which links to the lack of a defined definition for the term “erasure” in the GDPR, see the previous subsection). In another case, Telegram is seriously lacking in transparency about its decisions towards take-down requests from data subjects. The messaging app only has a transparency report published at https://t.me/transparency in case it discloses a user’s IP address and phone number to relevant authorities under a court order confirming the user is a terror suspect. Nonetheless, it is hard to deny Google's and Facebook's efforts to increase transparency regarding data erasure as they are examples of more responsible forms of liability that many other firms (such as Telegram) have yet to embrace. However, it is also critical to realise that these efforts are still not enough to ensure the fulfilment of RTBF for data subjects who are victims of IBSA.

Thirdly, the onus is predominantly on victims to track down their private sexual images online, contact the data controllers and persuade them to act on the abuse materials. This is critically troublesome because many victims are unaware that their intimate images are being published or only find out after the images after an extended period. Consequently, the time difference between distributing, discovering, reporting, and taking down the content can mean that abuse materials are already disseminated further afield. Furthermore, victims' or their authorised representatives' capacity to seek the protection they should receive can also be limited due to ambiguous guidelines, lack of transparency and unwillingness to collaborate. For example, a recent study by the Italian advocacy organisation – PermessoNegato – revealed “refractory” and “complacent” responses of Telegram to reports of IBSA (Cater, 2021). Henry & Witt (2021) further argue that by placing the responsibility on victims, these digital platforms might also inflict extra emotional, financial, and other burdens on already vulnerable women. The process can be lengthy, demanding, expensive too if the job is outsourced to a lawyer, and not guaranteed successful.

Responsibility to protect victims of IBSA

Through the years, IBSA has developed together with the advancement of technology. Given the rising power of technology providers both on individuals and on society as a whole, their influence on women’s rights cannot be overlooked (Coombs, 2021). Despite that, tech companies provide users

with little safeguards in terms of privacy, justice and equality (Witt *et al*. 2019). Thus, they need to take action to bridge the abuse happening on their platforms and "lead the way in providing better ways of supporting" victims in many ways (McGlynn *et al*., 2019). Henry & Witt (2021) further note that more state-based legislation is required to assist in better-integrating governance decisions by tech companies on the basis of social justice and human rights frameworks.

As analysed above, the current European data protection law is placing the power to control other people's lives in corporations' hands. Relying solely upon their judgements has been proven problematic for victims: in many cases, women's rights are not protected like how they are supposed to be. After all, effective responses need the collaboration of multiple stakeholders in order to exchange information and purposefully reflect lived experiences when making decisions (Coombs, 2021). The responsibility in protecting victims of IBSA does not only fall into digital platforms or governments. The service providers and the governments should collaborate with victims and their advocates to ensure adequate and comprehensive remedies and safeguard human rights, ultimately promoting social justice and ethics rather than just economic profit.

Conclusion

The paper analysed the opportunities and the challenges of applying the RTBF pursuant to the GDPR as a remedy for victims of IBSA. It is argued that the RTBF has the potential to protect victims from further harmful impacts caused by tarnished reputation, protect and promote their autonomy and privacy, and provide a legal support system for victims to reclaim their control. By recognising diverse needs and implementing victim-centred approaches, the legal system and service providers can help them regain a sense of control and empowerment to act in their best interests. Despite the potential of the RTBF, there is still a stark gap between the law and practice of platforms' governance in response to erasure requests from victims of IBSA. Specifically, the paper identified five main issues limiting this approach: (1) limited extraterritorial application of domestic law while dealing with transnational abuse; (2) ambiguous language about how data has to be removed; (3) problematic terminology in addressing IBSA that does not cover the nature of such abuse; (4) lack of liability fulfilments from digital platforms; and (5) lack of multi-stakeholder solutions tackling the abuse.

By examining the opportunities and challenges of the RTBF as a remedy for IBSA, this work presented a new problem with the potential to extend the research further. Victims of IBSA require inclusive and internationally relevant answers. They need to have a safe online space and the authority to make decisions that encourage recovery, rehabilitation, and unity. SVAW is becoming more and more challenging in this digital era, but we are falling behind in reactive and proactive remedies. Understanding the nature of IBSA, as well as the particular challenges that victims experience, could help design more compassionate, user-friendly digital places in the long term. After all, even if the RTBF as a remedy for IBSA might present many challenges in practice, it could still be a potential approach for the States and tech companies to adopt, leading to the development of more global and comprehensive solutions tailored for victims in the worldwide nature of the digital realm. The RTBF pursuant to the GDPR further sets an example for different jurisdictions across the world to develop their own rules that can address online abuse and protect individuals' privacy, leading to a global application of data protection rights without any geographical limitations. Given the complexity of this practice that crosses various fields of expertise and disciplines, further research on the human rights due diligence of the States and the internet intermediaries to protect and promote human rights

in different juridical contexts is needed if we want to build the foundation for a human rights-based digital space.

Declaration of Interest Statement

The authors declare that they have no conflict of interest.

References

Alexa Internet. (n.d.). *Alexa—Top sites*. Alexa. Retrieved 30 September 2021, from https://www.alexa.com/topsites

Cater, L. (2021, January 13). *How Europe's privacy laws are failing victims of sexual abuse.* POLITICO. https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/

Citron, D. K. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

Cook, L. (2015). The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law & Policy. *Journal of Law, Technology & the Internet*, 6(1), 121–132.

Coombs, E. (2021). Human Rights, Privacy Rights, and Technology-Facilitated Violence. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald International Handbook of Technology Facilitated Violence and Abuse* (pp. 475–491). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211036

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, 11(1), 100. https://doi.org/10.1186/1471-2288-11-100

Edwards, L. (2014, July 29). *Revenge porn: Why the right to be forgotten is the right remedy.* The Guardian. http://www.theguardian.com/technology/2014/jul/29/revenge-porn-right-to-be-forgotten-house-of-lords

Fabbrini, F., & Celeste, E. (2020). The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21(S1), 55–65. https://doi.org/10.1017/glj.2020.14

Facebook. (2020, August 21). Data Policy. Facebook. https://www.facebook.com/policy.php?ref=pf

Facebook. (2021a). Community Standards Enforcement Report—Adult Nudity and Sexual Activity. Facebook. https://transparency.fb.com/data/community-standards-enforcement/adult-nudity-and-sexual-activity/facebook/

Facebook. (2021b). Facebook Community Standards: Adult sexual exploitation. Facebook. https://transparency.fb.com/en-gb/policies/community-standards/sexual-exploitation-adults/

Facebook. (2021c). Facebook Community Standards: Manipulated media. Facebook. https://transparency.fb.com/en-gb/policies/community-standards/manipulated-media/

Goldberg, C. (2019, August 17). How Google has destroyed the lives of revenge porn victims. New York Post. https://nypost.com/2019/08/17/how-google-has-destroyed-the-lives-of-revenge-porn-victims/

Google. (n.d.). *Right to be Forgotten Overview—Legal Help*. Google Legal Help. Retrieved 5 October 2021, from https://support.google.com/legal/answer/10769224?hl=en#zippy=

Google Search Help. (2021). *Remove involuntary fake pornography from Google—Google Search Help*. Google Search Help. https://support.google.com/websearch/answer/9116649

Gutmann, A., & Warner, M. (2019). Fight to Be Forgotten: Exploring the Efficacy of Data Erasure in Popular Operating Systems. In M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, & A. Bourka (Eds.), *Privacy Technologies and Policy* (pp. 45–58). Springer International Publishing. https://doi.org/10.1007/978-3-030-21752-5_4

Henry, N., Flynn, A., & Powell, A. (2018). Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research*, 19(6), 565–581. https://doi.org/10.1080/15614263.2018.1507892

Henry, N., Flynn, A., & Powell, A. (2020). Technology-Facilitated Domestic and Sexual Violence: A Review. *Violence Against Women*, 26(15–16), 1828–1854. https://doi.org/10.1177/1077801219875821

Henry, N., & Powell, A. (2016). Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law. *Social & Legal Studies*, 25(4), 397–418. https://doi.org/10.1177/0964663915624273

Henry, N., & Witt, A. (2021). Governing Image-Based Sexual Abuse: Digital Platform Policies, Tools, and Practices. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald International Handbook of Technology Facilitated Violence and Abuse* (pp. 749–768). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211054

Hopkins, N. (2017, May 21). *Revealed: Facebook's internal rulebook on sex, terrorism and violence.* The Guardian. https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence

Intersoft Consulting. (n.d.). *GDPR: Right to be Forgotten.* Intersoft Consulting. Retrieved 13 July 2021, from https://gdpr-info.eu/issues/right-to-be-forgotten/

Johnson, B. (2019, March 25). *Deepfakes are solvable—But don't forget that "shallowfakes" are already pervasive*. MIT Technology Review. https://www.technologyreview.com/2019/03/25/136460/deepfakes-shallowfakes-human-rights/

Ku, R. S., & Lipton, J. D. (2010). *Cyberspace Law: Cases and Materials* (3rd ed.). Aspen Publishers.

Laville, S. (2016, April 11). *Top tech firms urged to step up online abuse fightback.* The Guardian. http://www.theguardian.com/technology/2016/apr/11/facebook-twitter-google-urged-to-step-up-online-abuse-fightback

McGlynn, C., Johnson, K., Rackley, E., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2020). 'It's Torture for the Soul': The Harms of Image-Based Sexual Abuse. *Social & Legal Studies*, 0964663920947791. https://doi.org/10.1177/0964663920947791

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, 25(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2

McGlynn, C., Rackley, E., Johnson, K., Henry, N., Flynn, A., Powell, A., Gavey, N., & Scott, A. (2019). Shattering Lives and Myths: A Report on Image-Based Sexual Abuse [Project Report: Durham University]. University of Kent.

Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2019). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, 92, 393–402. https://doi.org/10.1016/j.chb.2018.11.009

Prasad, R. S. (2019, November 6). *Ravi Shankar Prasad: India views its privacy seriously, data imperialism not acceptable.* The Economic Times. https://economictimes.indiatimes.com/tech/ites/india-views-its-privacy-seriously-data-imperialism-not-acceptable-ravi-shankar-prasad/articleshow/71937835.cms?from%3dmdr

Rackley, E., McGlynn, C., Johnson, K., Henry, N., Gavey, N., Flynn, A., & Powell, A. (2021). Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse. *Feminist Legal Studies*, 29(3), 293–322. https://doi.org/10.1007/s10691-021-09460-8

Reicherts, M. (2014, August 18). The right to be forgotten and the EU data protection reform: Why we must see through a distorted debate and adopt strong new rules soon [Text]. IFLA World Library and Information Congress, Lyon. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_14_568

Semenzin, S., & Bainotti, L. (2020). The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities. *Social Media + Society*, 6(4), 2056305120984453. https://doi.org/10.1177/2056305120984453

Statista. (2021). *Most popular messaging apps. Statista.* https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/

Stevenson-McCabe, S., & Chisala-Tempelhoff, S. (2021). Image-Based Sexual Abuse: A Comparative Analysis of Criminal Law Approaches in Scotland and Malawi. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (pp. 513–532). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211038

Suzor, N. P. (2019). *Lawless: The Secret Rules That Govern our Digital Lives*. Cambridge University Press. https://doi.org/10.1017/9781108666428

Svantesson, D. J. B. (2015). The Google Spain case: Part of a harmful trend of jurisdictional overreach [Working Paper]. https://cadmus.eui.eu//handle/1814/36317

Telegram. (n.d.-a). *Telegram FAQ*. Telegram. Retrieved 29 September 2021, from https://telegram.org/faq#

Telegram. (n.d.-b). *Terms of Service*. Telegram. Retrieved 7 October 2021, from https://telegram.org/tos

Telegram. (2021, March 24). *Telegram Privacy Policy*. Telegram. https://telegram.org/privacy#3-what-personal-data-we-use

Vincent, J. (2020, October 20). *Deepfake bots on Telegram make the work of creating fake nudes dangerously easy.* The Verge. https://www.theverge.com/2020/10/20/21519322/deepfake-fake-nudes-telegram-bot-deepnude-sensity-report

Witt, A., Suzor, N., & Huggins, A. (2019). The Rule of Law on Instagram: An Evaluation of the Moderation of Images Depicting Women's Bodies. *University of New South Wales Law Journal*, 557–596. https://doi.org/10.53637/ipmc9544

Appendix

Table 1: Overview of key elements in platform policies relating to IBSA erasure requests and responses of Google, Facebook and Telegram

	Google	Facebook	Telegram
Terminology			
- "image-based sexual abuse"	non-consensual explicit or intimate personal images, involuntary fake pornography, content about me on sites with exploitative removal practices	Sextortion, revenge porn, non-consensual intimate images	illegal pornography content
- "erasure"	remove, delist	erase	delete, take down
Victims can request IBSA content removal with the RTBF	x	x	x
Victims can request IBSA content removal without the RTBF	x	x	x/⃠[a]
Types of data erased	URLs to search results under data subjects' names (the data is still viewable after being delisted if using other search keywords)	any photos, videos in Facebook	"publicly viewable" photos, videos, chats (only includes public groups, channels, bots)
Territorial scope of erasure requests under GDPR	EU and EEA	worldwide	worldwide
Transparency report			
- Number of requests received	x[b]	x[c]	
- Number of requests accepted	x[b]	x[c]	
- Number of removed contents were appealed		x[c]	
- Number of deleted contents restored after appealing		x[c]	
- Number of deleted contents restored without appealing		x[c]	
- How data is erased			

[a] Telegram's policy is rather ambiguous in this regard.

[b] Google only gives the data of all requests under the RTBF since 2014 without clarifying specific reasons. No reports are provided for IBSA erasure requests outside the GDPR.

[c] The Transparency Report on Facebook is a periodical reporting system that provides "community insight" into how the platform enforces community standards, protects intellectual property, reacts to legal demands for user data or content restrictions, and monitors internet outages throughout the network, but no statistic is provided for requests under the GDPR.