PRIVACY E INNOVAZIONE

STUDI E RICERCHE SULLA PROTEZIONE
DEI DATI PERSONALI NELL'ERA DIGITALE

6

PRIVACY E INNOVAZIONE

STUDI E RICERCHE SULLA PROTEZIONE DEI DATI PERSONALI NELL'ERA DIGITALE

La collana ospita i risultati delle attività di studio e ricerca avviate o promosse dal Centro studi privacy e nuove tecnologie: monografie tematiche, paper e position paper che seguono l'evoluzione del tema della protezione dei dati personali in una prospettiva multidisciplinare (giuridica, politico–sociale, tecnologica) proponendo chiavi di lettura innovative. Sono inseriti in collana anche gli atti dei convegni organizzati dal Centro studi, gli interventi e i documenti presentati dai membri in occasione della partecipazione, in qualità di relatori, a conferenze e convegni. In "Privacy e Innovazione" sono pubblicate opere di alto livello scientifico, anche in lingua straniera, per facilitarne la diffusione internazionale.

Il direttore approva le opere e le sottopone alla revisione paritaria con il sistema del "doppio cieco" (*double blind peer review*) nel rispetto dell'anonimato sia dell'autore, sia dei due revisori che sceglie: l'uno da un elenco deliberato dal comitato scientifico, l'altro dallo stesso comitato in funzione di revisore interno. I revisori rivestono o devono aver rivestito la qualifica di professore universitario di prima fascia nelle università italiane o una qualifica equivalente nelle università straniere.

Ciascun revisore formulerà una delle seguenti valutazioni:

— pubblicabile senza modifiche;
— pubblicabile previo apporto di modifiche;
— da rivedere in maniera sostanziale;
— da rigettare;

tenendo conto della: a) significatività del tema nell'ambito disciplinare prescelto e originalità dell'opera; b) rilevanza scientifica nel panorama nazionale e internazionale; c) attenzione adeguata alla dottrina e all'apparato critico; d) adeguato aggiornamento normativo e giurisprudenziale; e) rigore metodologico; f) proprietà di linguaggio e fluidità del testo; g) uniformità dei criteri redazionali. Nel caso di giudizio discordante fra i due revisori, la decisione finale è assunta dal direttore, salvo casi particolari in cui questi provveda a nominare tempestivamente un terzo revisore a cui rimettere la valutazione dell'elaborato. Il termine per la valutazione non deve superare i venti giorni, decorsi i quali il direttore della collana, in assenza di osservazioni negative, ritiene approvata la proposta. Sono escluse dalla valutazione gli atti di convegno, le opere dei membri del comitato scientifico e le opere collettive di provenienza accademica. Il direttore, su sua responsabilità, può decidere di non assoggettare a revisione scritti pubblicati su invito o comunque di autori di particolare prestigio.

Elisabetta Stringhi

"Revenge porn" on on-line platforms: legal interpretations and approaches to combat non-consensual intimate image distribution

Preface by
Pierluigi Perri

aracne

ISBN
979-12-218-0593-2

first edition
roma 3 April 2023

I never walk alone at night, and I get chills when I catch someone staring at me.
I always wonder to myself, 'are they staring at me because they recognize me from the Internet?'

Danielle Keats Citron[1]

[1] CITRON, D. K. *Hate Crimes in Cyberspace*, Harvard University Press, 2014, p. 48.

Table of contents

Preface

Prof. Pierluigi Perri[1]

The topic of this book is becoming increasingly important in the analysis of the relationship between human beings and technologies, especially when this relationship leads to the so-called cyberviolence, which unfortunately affects vulnerable people, women and minors, to a greater extent.

While, on the one hand, one of the advantages offered by modern communication technologies consists precisely in the possibility of constantly flowing of information among different users, on the other hand, the possibility of being always connected and reachable has led to forms of digital violence that no longer know boundaries of space and time[2].

Now, on the other hand, the pervasiveness of technologies allows us to be always connected and to be, therefore, always potential victims of some action conducted to create some kind of damage against us, which could in some cases even constitute a crime.

I am referring, of course, mainly to the phenomenon of social media[3], which in various forms and expressions continues to

[1] Pierluigi Perri is an Associate Professor of «Information Security, Privacy and Protection of Sensitive Data» at the University of Milan.

[2] In past times, in fact, phenomena such as bullying, hate speech or the non-consensual collection of images or conversations found a limit in the need to be in a specific physical location in order to be affected by them, or in the limited possibility of disseminating offensive, discriminatory or personally damaging content in a social sphere, which was by design more restricted.

[3] It is interesting, however, to note that since the beginning Internet and the Web were designed more as a social creation than a technical one. See T. Berners-Lee, Weaving the Web. The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor, HarperCollins, 2000, p. 123

represent the main mode of use of digital tools. Through it, in fact, users can disseminate content in various ways (texts, images, videos, voice recordings) reaching an indefinite number of people who, in turn, will be able to repost the same content transmitting it and thus allowing its absolutely uncontrolled dissemination.

It is precisely in the inability to control a content that lies the danger of information posted on social networks. Indeed, the persistence of the latter exposes the victims to a constant risk of seeing themselves published, shared, denigrated or otherwise depicted in situations not intended to be disseminated to third parties.

This cyberviolence has different declinations, many times identifiable in behaviors that are already punished as crimes, but in which technology plays a fundamental role because it allows to amplify the negative effects of those behaviors.

In particular, as has already been pointed out, digital contents have the ability to overcome classic "safety" barriers such as the domestic walls, or the ability to never completely disappear, but to be able to suddenly re-emerge causing the victim to suffer again the same bad experience, with the knowledge that this situation could never come to an end even in years.

Further complicating this picture, as will later be explained in this book by the Author, are the emerging technological developments that amplify already terrible behaviors even more. The phenomenon of the deep fake is an example of how technology, when used in a distorted way, can create problems rather than solve them. Thanks to these applications of artificial intelligence, in fact, it is possible to portray a person within a given context or while performing actions that, however, he or she never actually did. This has been used, for example, to replace the image of the face of some women to actresses performing in pornographic contents and then spread them on the Web. In today's society, which is characterized by the sharing of content and the possibility for anyone to comment on that content, the damage to the dignity of subjects portrayed in situations they have never experienced, with respect to which

even the activity of disallowing the footage requires special (and expensive) technical analysis, becomes even more profound.

Faced with such a picture, it is clear that the response must be complex and appropriate to a fluid landscape such as the technological one. Indeed, a purely technical response, such as forbid certain technologies, or a purely legal one, such as tightening sanctions related to certain behaviors, would risk being inefficient.

This has been realized by the various continental "blocs", which are addressing the problem consistently with their legal traditions and fundamental rights protection, considering that they are inevitably threatened by such events.

In fact, as a technological response, tools for detecting and remove illicit content are being refined, keeping in mind, however, that this practice is not without problems and could in turn infringe on fundamental rights, first and foremost freedom of expression. It is unavoidable, in fact, that such forms of preventive control will necessarily have to be automated (at least in part), and this could lead to a series of false positives that would have the effect of removing lawful content or shutting down accounts of completely unsuspecting users, with the subsequent difficulties of rehabilitation to the platform.

Also from a technological standpoint, investigative digital forensics techniques are also being refined, through which is possible to identify the source of the illicit content and, presumably, the author. The alleged anonymity that can be achieved on telematic networks, in fact, is among the main causes that justify the proliferation of such behaviors. If digital investigation techniques were to evolve to the point where perpetrators of these offenses would not go unpunished, the phenomenon would probably know a lesser extent.

In this sense, the Volume also analyzes in depth the interventions of some international bodies such as the Council of Europe, which have devoted much of their energies in the framing of the different phenomena (cyberbullying, revenge porn, deepfake, etc.) and on how the already existing international conventions can also be used to counter these

phenomena , including with regard to the collection and use for investigative purposes of the digital evidence[4].

From the point of view of law, actions are moving on two different planes, which could be summarized in the enforcing of laws aimed at correctly framing the cases and leading back to a sanction, most often criminal, but also empowering Supervisory Authorities so that they can immediately intervene with providers and remove illicit content.

The Italian Garante per la protezione dei dati personali, in particular, is increasingly active in reporting and coordinating with ISPs so as to prevent certain non-compliant processing of personal data from harming users, especially when those users belong to weak categories such as minors or women. To this end, the Garante is carrying out an extensive information campaign against these phenomena to increase user awareness, which remains the first tool of defense, but it is also intervening with providers so that they cooperate both in the prevention phase with respect to the uploading of illicit content and in the phase of timely removal of this content.

According to the current President of the Garante, Prof. Stanzione, it is indeed necessary to:

(a) make remedial protection effective, especially in a specific form (removal in particular), which also makes it possible to limit the effects of the permanence of harmful content on the web, preventing its aggravation;

b) empower users and providers, while ensuring easier means of identifying the authors of offensive content;

c) investing in "digital pedagogy" as awareness, on the part of all web users, of the often irremediable implications that each of their clicks has on the dignity of human beings, even if dematerialized behind a social profile.

To this educational approach, one can add the tools proper to the General Data Protection Regulation and by the Legislative

[4] Cfr. the T-CY Mapping Study on Cyberviolence drafted by the Budapest Convention Committee of the Council of Europe and available at the following URL: https://rm.coe.int/c-proc-webinar-introduction-to-cyberviolence-june-2020-t-cmapping-st/ 16809ebc79.

Decree 196/2003, in particular the specific powers attributed to the Garante[5] and the rights of the data subject - such as the right to deletion - which provide a legal action for every person involuntarily portrayed in intimate situations or otherwise threatening his or her dignity, to act directly towards the gatekeeper of the content and ask for its removal and subsequent control so that this content does not recur.

The Volume illustrates in a comprehensive and scientifically precise way this framework and the underlying complexities, but it also does not fail to offer some critical insights, particularly with regard to some proposed regulations currently under discussion in the European Commission, where a more decisive intervention of the legislator would have been desirable to counter some criminal phenomena, especially when related to Artificial Intelligence, which daily shows its growing capabilities and consequent concerns for the rights of human beings.

The reader, however, will not lack food for thought and this certainly represents an excellent result already achieved by the Author, who will provide with her critical reconstruction some indispensable elements to understand what is endangering our future and our rights.

[5] See for example Article 144-bis of Legislative Decree 196/03 specifically regulating the procedure for preventing the spreading of revenge porn contents.

Introduction

New forms of technology-facilitated violence are emerging online and facilitated by the use of information and communication Technologies (henceforth "ICTs"), thus representing a global concern. The fast digital and technological development, including the rapid evolution of Artificial Intelligence (also "AI"), 5G and the Internet of Things ("IoT") will inevitably give rise to new and different forms of cyberviolence, with serious individual and collective implications worldwide.

A comprehensive definition of the phenomenon of cyberviolence will be further provided in this Introduction. As will be shown below, while cyberviolence is undoubtedly a comprehensive phenomenon targeting numerous categories of victims, regardless of gender and age, it is true that cyberviolence against women has its own specific characteristics.

According to a 2016 survey, 53% of women experienced harassing behaviours online versus 40% of men in the U.S.[1] The European Institute for Gender Equality stated that one in ten women have already experienced a form of cyber violence since the age of 15[2]. As reported by a study conducted for Amnesty International, 23% of women has experienced abuse or harassment online on one or more occasion, with significant social and psychological consequences[3]. According to said

[1] DATA AND SOCIETY RESEARCH INSTITUTE, *Online Harassment, Digital Abuse, and Cyberstalking in America*, New York, 2016.

[2] EUROPEAN INSTITUTE FOR GENDER EQUALITY, *Cyber violence against women and girls*, 2017.

[3] IPSOS MORI, *Online abuse and harassment*, 2017.

studies, women appear to be disproportionately targets of certain forms of cyberviolence compared to men. Therefore, part of the gender studies literature on ICTs and cyberviolence claims that everyday women's online experiences differ from the ones of men. However, as reported in a study conducted on 2.000 Italian respondents[4], the male presence among victims is more important than one could commonly think, as it amounts to the total 30% of the sample. Approximately half of this percentage is part of the LGBTQ+ community (13%).

A wide array of different terminologies are used to describe cyberviolence, including "cyberhate", "technology-facilitated violence", "tech-related violence", "online abuse", "hate speech online", "digital violence", "networked harassment", "cyberbullying", and "cyberharassment". Cyberviolence against women is also defined as "online violence against women" and "online misogyny"[5]. As poignantly pointed out, online misogyny is a cultural broad notion that captures the effects of online abuse beyond violence, such as chilling, silencing and self-censorships effects on women and girls in the political landscape of the online culture wars. In other words, cybermisogyny is "*an umbrella term for all kinds of negative experiences that women can go through online because of their gender*"[6].

To correctly frame cybermisogyny, it is worth examining the "manosphere" culture. Otherwise, the phenomenon could be wrongly underestimated and dismissed as mere individual hostility or as the result of frustrated "trolls"[7]. On the contrary, the "manosphere" culture is the result of the advent of social

[4] THE FOOL, *Revenge Porn Research,* 2020.

[5] D. GING, E. SIAPERA, 2018. "Special issue on online misogyny". *Feminist Media Studies*, 18 (4), pp. 515-524.

[6] D. GING, E. SIAPERA, *Gender Hate Online: Understanding the New Anti-Feminism*, Dublin, Palgrave Macmillan, 2019.

[7] A "troll" or "trolling" are Internet slang terms referring to the person or the act of posting deliberately inflammatory and provocative messages intended to produce a large volume of frivolous responses, to get attention and to disrupt substantial conversations. Definition of the Collins Dictionary, at: https:// www. collinsdictionary. com/ dictionary/ english/ troll. See also Z. WILLIAMS, 2012. What is an Internet troll? The Guardian, 12 June. Available from: https://www.theguardian.com/technology/2012/jun/12/what-is-an-internet-troll.

networking and its subcultural groups who amplified and polarised gender politics in an ongoing cultural conflict[8], within a wider cultural landscape online and offline.

'Manosphere' is a portmanteau of the English words "man" and "sphere". Authors define the phenomenon as an aggregate of different communities who share a common language and are orientated against the rhetoric of feminism and, broadly, gender-equality[9]. Throughout this context, denial and conspiratorial thinking are commonplace.

Manosphere embraces several categories of different users, including: 'Men's Rights Activists' (MRAs)[10], 'Men Going Their Own Way' (MGTOW)[11], 'Pick-Up Artists' (PUA)[12],

[8] Cit. D. GING, E. SIAPERA, 2018, *op. cit,* pp. 515-524.

[9] A. E. MARWICK, R. CAPLAN, (2018). "Drinking male tears: language, the manosphere, and networked harassment". *Feminist Media Studies*, 18(4), pp. 543-559.

[10] "Men's Rights Activism" (henceforth MRA) appeared online in the 2010's as a reaction to feminism, subsequently spread worldwide on the Internet. Some members are concerned with calling due attention to men's issues, such as depression, suicide rates, homelessness, however the majority rather tends to violent misogyny. Their action exploits "memes", a cultural element that is repeated, shared, parodied and copied, for advertisement and propaganda purposes. It is growing as a social movement across different cultures and geographies, aggregating around a common ideological background founded on anti-feminist and misogynistic discourse. See cit. D. GING, E. SIAPERA. *Gender Hate Online: Understanding the New Anti-Feminism*, *op. cit.,* p. 89.

[11] "Men Going Their Own Way" (henceforth MGTOW) is a manosphere subculture revolving around the main concept that contemporary romantic relationships are intrinsic threatening for a social and cultural landscape that is male-biased. According to this view, men are accounted for social and relational failures or conflicts, such as in family litigations or in sexual assault prosecutions, therefore leading to a lifestyle of occasional encounters or, even, celibacy. See for instance a MGTOW forum discussion: https://www.mgtow.com/forums/topic/why-false-rape-is-far-worse-than-rape/.

[12] The Pick-Up Artists (henceforth PUA) is an online subculture consisting of members who share suggestions on the art of seduction, a phenomenon that exploded in 2005 due to the publication of the book *The Game. Penetrating the Secret Society of Pick-up Artists or The Game. Undercover in the Secret Society of Pickup Artists* by the investigative reporter Neil Strauss. Far from confining exclusively in the virtual sphere, the community often manifests offline, for example by organizing dating seminars that legitimate psychological manipulation and even physical violence. A notorious case regarded the PUA Julien Blanc, accused of promoting sexual assault and violence against women, banned from entering the United Kingdom. See A. TRAVIS, 2014. Julien Blanc banned from entering UK. The Guardian, 19 November.

'InCels'[13], 'Gamers'[14] and Alt-Right advocates[15]. "Bomberismo" and "Pastorizia" are examples of the Italian manosphere[16]. Although different, gender scholars claim that all these categories perform forms of cyberviolence against women, with the ultimate dissolution of private and public boundaries, between domestic and public violence, in a continuum of online and offline violence[17].

Cyberviolence includes, without limitation, verbal abuse, sexual harassment, doxing, spamming, denial of access, hacking or cracking, surveillance, tracking, impersonation, mobbing, trolling attacks, "brigading", hateful speech, extortion, sextortion, intimidation, rape, lynching and death threats, cyber-stalking, creepshots, upskirting, digital voyeurism, photo-manipulation such as memes, non-consensual pornification and

[13] The term "InCel", as a portmanteau of the English words "involuntary" and "celibacy", refers to men who believe that, for reasons beyond their control, they are destined to remain celibate, in a so-described state of "inceldom". The InCel community, through the development of archetypical figures and misogynist rhetoric, accuses women for their incapacity to find sexual or romantic partners, this linked to feelings of self-loathing, low self-esteem, and outward-directed rage.

[14] "Gamers" refers to a part of the online gaming community who engage in misogynistic attacks and harassment. By way of illustration, the harassment campaign conducted via the hash tag #GamerGate forced game developer Zoe Quinn and video-game critic Anita Sarkesiaan to leave their homes, after calling for gender equality in the community. See the report PEW RESEARCH CENTRE, *Online Harassment*. Washington, DC, 2014.

[15] The "Alt Right", or "Alternative Right", constitutes a kind of identity politics from the right, focusing on the preservation of an ethnically "pure" society, therefore contrasting feminist instances for the biological and cultural reproduction of this identity. Come to the fore during the 2016 U.S. presidential elections, the movement mainly lives online. See G. HAWLEY, *Making Sense of the Alt-Right*, New York: Columbia University Press. 2017.

[16] "Bomberismo" refers to a sexist and xenophobic online subculture grounded on a simplified vision of society, by taking notorious football players as role models ("bomber" is the footballer detaining high score rates). "Pastorizia" constitutes a correlated online subculture that emphasises the lack of culture and education as "old time values" to be preserve and exalt.

[17] Liz Kelly first ideated the concept of the "continuum of violence" in 1987, according to which all forms of male violence against women are intertwined and form a continuum of violence.