Internet and Communications as elements for CIDT and Torture. Initial reflections in an unexplored field*

Pau Pérez-Sales, Laia Serra*****

The internet was once seen as a new and definitive window to freedom and a world without torture. There is however, another less obvious but perhaps more notorious side: torturous environments can also be created through the internet; a place where individuals may be targeted for discrimination, coercion or control. There is a dearth of academic research and theoretical developments in this very new area of knowledge and this Editorial will review and reflect on various aspects, thereby suggesting possible lines of research.

Searching for definitions

A recent theoretical review in the field of online violence (Harris & Woodlock, 2019) with its focus on gender, proposed the use of the term *technology-facilitated coercive control* when referring to abuse using social networks or the internet. The authors propose that similar denominations are sought for other kinds of digital violence and suggest that any denomination of these new phenomena include the terms perpetrator and purpose. Other expressions found in the literature include *digital coercive control* (DCC), *technology-facilitated violence* (TFV), or *technology-related violence* (Douglas, Harris, & Dragiewicz, 2019).

The Council of Europe's Cybercrime Convention Committee has recently defined cyberviolence[1] as: "*the use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities"* (T-CY, 2018), a definition also adopted by the European Parliament (Van Der Wilk, 2018).

This definition, however, focuses on the internet and leaves aside other forms of communication. For the purposes of this editorial, we will consider a wider perspective and, mirroring the conditions of the UNCAT definition, consider Internet and Communications Ill-Treatment and Torture (ICIT) as *those acts of violence intentionally committed, instigated or aggravated, in part or whole, by the use of information and communication technologies that cause psychological and emotional pain or suffering, for such purposes as obtaining informa-*

*) The Editor-in-Chief takes full responsibility for the content of the Editorial. The opinions expressed are his own and do not necessarily reflect the view of the Publisher.
A draft version of this Editorial was used and mentioned in the UN Special Rapporteur on Torture Report (2020) A/HRC/43/49 on Psychological Torture, as entitled "Internet and Torture".

**) Editor-in-Chief.
Correspondence to: pauperez@runbox.com

***) Criminal lawyer specialising in gender, digital violence and freedom of expression.
Correspondence to: laiaserra@icab.cat

1 https://www.coe.int/en/web/cybercrime/cyberviolence#{%2250020850%22:[0]}

https://doi.org/10.7146/torture.v30i1.120593

tion, punishment, intimidation, coercion or for any reason based on discrimination of any kind when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.

This is achieved, among other methods, by inducing emotional suffering through threats and fear, breaking bonds of confidence in the targeted person, inducing shame, embarrassment, humiliation or guilt, promoting and fostering prejudices and discrimination, damaging reputation, creating conflict with peers, fellows, relatives or loved ones or breaking community ties. The ultimate objective, as in classical torture, would be to change the identity, attitudes or behaviours of the targeted person and break their will. These are working definitions that need to mature further, as research and knowledge develops.

A particular challenge relates to the role of the state in ICIT. Indeed, a state's passivity or lack of due diligence, when acting against recurring and known patterns of digital violence, especially those affecting socially discriminated groups such as women or social or politically-motivated activists, facilitates ICIT's alignment with the classic definition of torture or ill-treatment. In her 2018 report, the United Nations Special Rapporteur on the issue of violence, its causes and consequences, stated that the duty of due diligence to prevent, investigate and punish sexist violence, extends to the digital world (UN Human Rights Council, 2018).

Medical and Psychological Impacts.

Although there are no studies on the level of psychological pain that ICIT can entail, future studies in this new field must consider at least three sources of suffering: (a) direct effects: fear, shame, guilt, helplessness or rage, leading to anxiety, depressive or somatisation disorders (b) indirect effects: the cognitive and emotional burden of being forced to devote time and energy to prevent and counteract such acts (i.e. to defend reputation publicly, assess danger and implement eventual security measures or to try to circumvent surveillance and control) (c) psychosocial effects: impact on family, interpersonal relationships, workplace and social networks (i.e fear, detachment, polarisation, rumour spreading…).

The closest reference in academia is cyberbullying[2], and digital dating abuse[3], although the severity of threats, danger and degradation is not comparable to that of ICIT and there is no consensus on the role of the state. A recent European Transnational Study with more than 5000 respondents found three profiles of emotional consequences: 5% of teenagers showed severe emotional damage to cyberbullying including suicidal tendencies; for 75% of teenagers, there were moderate symptoms of anxiety or depression that disappeared with time and 20% cyberbullying had no major impact on them (Ortega et al., 2012). A review of the specific relationship between suicide attitudes and cyberbullying using studies from 1997 to 2018, found that those who experience cyber victimisation are at two to three times more risk of committing suicide[4] depending on personal and social vulnerability factors that themselves would necessitate further exploration (John et al., 2018). Although these are

2 There is no consensual definition of bullying and cyberbullying. For a review of definitions see Gleeson (2014). Bullying is defined as *ongoing harmful behaviour in relationships with power disparities*. Cyberbullying is referred to the use of communication technologies for bullying.

3 Digital dating abuse is defined as *the use of verbal, physical and sexual aggression by an intimate partner*.

4 OR 2.35 (95% CI 1.65-3.34) times as likely to self-harm, OR 2.10 (95% CI 1.73-2.55) times as likely to exhibit suicidal behaviors and OR 2.57 (95% CI 1.69-3.90) times more likely to attempt suicide

indirect data obtained from a population comprising different ages and in different contexts, it highlights the immense mental suffering that Internet and Communications Ill-treatment and Torture can entail.

Certain organisations track internet-related violence specifically as a form of gender-based violence (Barrera & Rodríguez, 2017; Serra, 2018; Van Der Wilk, 2018). Especially relevant is the work of Colectivo Luchadoras ("Fighters Collective") from Mexico (Barrera & Rodríguez, 2017); a feminist group that has collected and analysed hundreds of internet incidents and propose 13 categories that could serve as a good point of departure for the academic study of ICIT (table 1).

There is also a similar classification developed by the Internet Governance Forum (IGF, 2015).

Summarising table 1, the Internet Governance Forum and the Council of Europe documents, we can consider four main situations: (a) Coercion, threats, and intimidation; (b) Surveillance, monitoring, and control in real-time; (c) Theft of sensitive information; (d) Defamation and public degradation.

In terms of analysis, and from a psychological perspective, conditions (a) and (b) are fear-producing actions, and (c) and (d) target identity.

Essential elements to understand Internet and Communications related-violence as ill-treatment or torture.

We have defined internet related violence. Now, we turn to the subject that suffers this violence and to a new phenomen: the difficult to define new identities.

Internet-based identities.

ICIT has peculiar characteristics that derive from attacks on new forms of identity created through the internet, the exact definition of which is still subject to debate. *Digital identity* is defined as that which a person creates on the internet by constructing a way of presenting him or herself in the virtual community (Gonzales & Hancock, 2011). A related concept is *Information Technology (IT) identity*, as the extent to which an individual views IT as integral of a person's sense of self -as both a new type of material identity and an integral part of the self (Carter & Grover, 2015). There is however, an even more under-researched identity: the identity that others (including the state) create of us. When others (including the state) create and spread information about us, inaccuracies blend seamlessly with the truth, the totality of these elements making up the image others have of us (our "digital identity"). Anyone carrying out a web search will be unable to distinguish true elements from those that may be defamatory and will likely make conclusions based on the totality of what is found. Our digital identity is, as a result, almost impossible to control. The higher the levels of exposure, the higher the risks of losing control. It is not surprising that those growing up in the era of new technologies, who are much more conscious of their new digital identity, devote time to carefully construct their *digital self.*

Furthermore, amongst consistent users of social networks (as is the case with many human rights activists), there is a dialogical effect: the internet constitutes a distinctive "looking glass" that modifies one's identity (Zhao, 2005) and research shows that the more it is used, the more vulnerable a person is to what others say about them (Manago, 2014). Stigma in the form of a permanent digital footprint is arguably more difficult than ever to escape. The internet has become a digital prison (Lageson & Maruna, 2018) by producing a lasting mark of shame through messages, comments, videos and/or pictures. That is very difficult to delete.

Table 1. *Mapping Internet and Communications attacks*

1. **Unauthorised access (tapping) and monitoring access.** Password theft, spyware; intervention/ tapping devices; equipment theft; locking user access; phishing[1], virus infection; key loggers[2].
2. **Control and manipulation of personal information.** Deleting, changing or falsifying personal data (photo or video); taking photos or video without consent (not necessarily with sexual content); controlling accounts on digital platforms.
3. **Spoofing and Identity Theft.** Creation of false profiles or accounts; usurpation of a personal website with name or data referring to the individual; impersonating an individual , including using your account to communicate; theft of identity, money or property.
4. **Monitoring and Cyberstalking.** Surveillance or hidden cameras, location identification employing images; geolocation on equipment /cellular or notifications; cyberfollowing; cyberstalking[3].
5. **Discriminatory statements.** Abusive comments; discrimination against various groups, electronic insults; discriminatory media coverage.
6. **Harassment.** Stalking; waves of group insults; messages from strangers; repeated messages; sending unsolicited sexual pictures.
7. **Threats.** Messages, images or videos with threats of physical or sexual violence
8. **Dissemination of personal or intimate information without consent.** Sharing private information (doxxing[4]); exposure of sexual identity or preference that generates risk (outing); dissemination of intimate or sexual content without consent; disclosure of privacy.
9. **Blackmail.** Sextorsion[5].
10. **Discrediting.** Dissemination of content; smear campaigns; defamation; disqualification.
11. **Technology-related sexual abuse and exploitation.** Deceiving for purposes of trafficking; sexual abuse; grooming[6].
12. **Attacks to channels of expression.** Removal of profiles or pages on social networks; DDOS attacks[7]; restrictions of use domain; domain theft; blackouts (from the state or company) during a meeting or protest or from a provider
13. **Omissions by actors with regulatory power.** Lack of regulation or implementation of protection measures related to messages, images or videos with threats of physical or sexual violence.

1 A technique that seeks to trick people into infecting and/or stealing information from a digital device.
2 Keylogg: Software or hardware that can intercept and save keystrokes on the keyboard of an infected computer.
3 The use of digital technology devices, or online activity, to monitor a person and to use the information harvested to harass or intimidate him or her online, to monitor his or her physical movements, or to capture him or her at a specific geographical location.
4 Doxxing: An abbreviation of the phrase "dropping docs," which refers to the act of sharing someone's personal details with others online, in particular a physical address or personal identification documents, such as a form of bullying or harassment.
5 Sextorsion: The use of intimate images or personal information as a form of coercion for sexual exploitation or blackmail
6 Grooming: The use of social networks to deliberately cultivate an emotional connection with minors for the purpose of sexual abuse or exploitation
7 DDOS attack: DDoS- Distributed Denial of Service – a malicious attempt to create massive traffic, resulting in temporarily or indefinitely disrupting service of a host connected to the internet

Internet and Communications Ill-treatment and Torture aims to provoke silence (Basak et al., 2019), but psychological and psychosocial mechanisms that operate between victims and perpetrators and between both and the wider digital community is also a field of academic research in its infancy. Anonymity and the search for popularity play a hitherto mediational role in these mechanisms. As an example, a recent study showed that a vast majority of shamers on Twitter shamed the victim and not the perpetrator. Shamers' follower counts also were seen to increase faster than that of the non-shamers, showing that shamers could easily be enticed to do so if their actions are validated by others (Basak et al., 2019). The mechanisms operating in the physical world are not the same that operate in the digital world. This was seen in a visionary manner by Guy Debord (1967/1995) in *The Society for Spectacle*, a book written before the digital era but essential to understanding some of the paradoxical destructive dynamics of the digital world.

Physical world

Outside of the context of the internet, the challenges are also vast. We live in what has been labelled a "post-privacy" world (Busch, 2019). Human beings are permanently exposed to scrutiny. Computers record personal interests, searches, purchases, sexual perversions or political ideology; gadgets capable of playing music and informing us of the weather are also capable of informing others of our preferences and conversations; phone applications access our photographs and videos; GPS and cameras inform on who we are and where we are; surveillance cameras in streets, banks and buildings can trace our paths and who we talk to or even what we say; credit cards and shopping apps record our steps and our tastes, while aerial cameras and drones allow tracking of individuals even in the middle of crowds. No news or event takes place, even in the most remote of places that is not recorded on smartphones, uploaded and viewed worldwide within a few hours, while Periscope, Instagram or Facebook also broadcast our lives. This is part of what big data analytics will provide to governments and private companies. It can however, also be used against individuals.

The power of big data analytics for social control is exemplified by the recent scandal involving the use of millions of Facebook profiles by Cambridge Analytica in London, to create psychological clusters of voters that were latterly used to further Donald Trump campaign[1]. Linked to this is the new academic branch of neuro-politics that studies how to control and direct voters by studying public and private brain responses to political stimuli (Rose & Abi-Rached, 2014; Schreiber, 2017).

Torture and ICIT

From a moral and ethical point of view, torture is defined relationally. It is grounded in concepts of *autonomy, control, and free will*. For philosophers and specialists in ethics, torture is a relationship between two human beings characterised by a violation of dignity and understood as a lack of recognition and respect, and a violation of autonomy, expressed by the absolute power, control and imposition of the will of the perpetrator, and the lack of control, powerlessness and suppression of the free will of the victim (Koenig, 2013; Luban, 2009; Maier, 2011; Parry, 2003; Pollmann, 2011; Scarry, 1985; Sussman, 2006).

When developing the idea of torture as related to dignity and humiliation, and the absolute repression of free will, most philosophers conceive of a one-to-one relationship between

1 https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

perpetrator and victim. The torturer aims to break the victim by, among other elements, attacking the victim's identity through fear and humiliation, which in turn produces emotional pain and suffering. In psychiatry however, humiliation is conceptualised as an interpersonal emotion. Torture survivors often have long-lasting feelings of humiliation and can perfectly recall the event or series of events when this humiliation was provoked by the perpetrator(s) and indelibly engraved in their memory.

Internet and communications-related violence acts exactly on these same two essential points, but with very particular distinctions.

1. *Fear is unspecific*. For the psychological study of fear as an emotion, there are two very distinct phenomena. Fears that are related to concrete and visible threats (i.e. an animal attacking the person) and fears related to invisible, unpredictable or unknown threats (i.e being confined in a dark place). While visible and predictable threats allow for some sense of control, invisible and unknown threats induce helplessness and despair (Hopper & Hidalgo, 2006; Phillips, 2011). ICIT is a modality of torture that (a) does not require the physical presence of a perpetrator, and in which (b) the perpetrator is quite often anonymous or behind a hidden or false identity[2]. Furthermore, both elements make it more difficult to demonstrate the link of the perpetrator with state actors or to make evident the political or discriminatory purpose of the threat.
2. *Shame instead of humiliation.* While humiliation happens in a private space between two persons or between a person and a small group of perpetrators, broadcasting through social networks means that the attack on an individual's identity happens in the public sphere, and is thus amplified and prolonged endlessly by the almost infinite memory of internet search engines (Hodalska, 2019). It is this condition of *public debasement* that makes *shame,* and not humiliation, the core emotion. From a psychological point of view, shame is more damaging and produces more pain and suffering than humiliation. While humiliation drives to action towards the perpetrator (rage, pursue of justice, sometimes desire of revenge), shame is usually linked to inhibition, paralysis, powerlessness, helplessness, avoidance of exposure and the desire to hide and disappear (Leary & Tangney, 2012).
3. *Cruelty.* Studies in social psychology show that the two most accurate predictors of cruelty in perpetrators are anonymity and impunity (Anderson & Carnegey, 2004). Experimental models show that when perpetrators are able to act without revealing their identity, they choose the most cruel actions possible. The same occurs when perpetrators can act with impunity and where retaliation is impossible. Cruelty is also further facilitated by the way that interaction takes place on social media and by the design and format of communication, such as limitations to the number of characters in posts that tends to provoke brief insulting messages.
4. *Mediated interaction.* If the purpose of torture is to control and break will, it is

2 As a side note, according to Douglas, Harris, & Dragiewicz (2019), to understand the emotional suffering of internet-related violence, the most essential variable is Spatiality. In their view the experiences of, risk and mental health consequences faced by victim/survivors in regional, rural and remote locations or where the perpetrator might physically reach the person are entirely different from pure on-line threats and must be studied separately.

essential to be able to see the impact of torture on the victim directly. In ICIT, quite often, there is an inability to see a victim's reaction (i.e. regarding threats to life). This can either protect the victim or trigger escalation. But there are also contexts in which visibility is clear and immediate; the victim's reaction is especially visible on the internet either through the violence that the victim explicitly shows as a reaction, or because the Internet community can perceive that the person attacked reduces online presence, maintains a "low profile", avoids interacting with certain profiles, loses followers or begins to be targeted by more and more parties.

5. *Permanent stress.* In ICIT, the perpetrator often has 24 hours uninterrupted access to the victim. The victim may engage in frequent checking behaviours with exponential anxiety and feelings of fear. Furthermore, each time violent or controversial content is reactivated, the trauma is also reactivated. Not knowing when the controversy may be revived generates a great deal of helplessness and a sense of vulnerability. It may also occur at a time when the victim is ill, emotionally fragile or facing other personal challenges, or equally at a time of professional growth that may suffer detriment as a result.
6. *Multiplicity of aggressors*. The impact of digital violence often does not originate from a single source. Instead, we witness either a snowball phenomenon with the multiplication of an initial violent content, or an organised collective attack in which the victim is confronted with the ripple effect of being violently targeted from different online profiles, at the same time and for the same reason. These two dynamics increase the feeling of helplessness, the inability to activate personal resources and the loss of self-esteem to the extent that it may irreversibly damage self-perception and identity.

These are six very specific and peculiar elements that make ICIT a condition liable to produce very severe pain or suffering, deserving specific studies from academia that have, at the time of writing, not yet been explored.

From theory to practice: ICIT cases

Threats and punishment

A nurse works in the health center of a rural community or a peripheral neighborhood. She provides clinical care to everybody in her community, including injured demonstrators who are participating in protests against the government. Some of her neighbours whose ideology aligns with the government inform the authorities, and she is, sometime in the future, made redundant by her employer. The government - like most current governments - has an agency that specialises in network monitoring and control. They soon find her presence on Facebook and in WhatsApp groups that disseminate, among other things, news they deem to be anti-government. She is thus put on a blacklist and considered an enemy of the state. Using false or anonymous IP addresses, the government agency floods other social networks connected to her (in particular her Twitter and Facebook family contacts), and networks akin to the government with messages that present her as a terrorist, as an anti-patriot and a danger to the community. They also reveal information to the media of an intimate or deeply humiliating nature from her time at university; something she thought that belonged to the past. The message is widely distributed and includes photos in which she is easily recognisable. A photo collage makes her appear to be holding a small weapon – which

she is not. As a consequence, pro-government groups begin to harass her, both inside and out of her new workplace through threats, insults or paintings on walls reproducing Twitter messages. She is terrorised, and despite her initial resistance and her efforts to delete all her social media accounts, the campaign becomes widespread and all her family and peers circles take positions on what they understand to be her ideological and personal viewpoints. She soon begins to think that there is a risk of direct physical aggression by organised groups, and eventual arrest by authorities. She is recognised by some patients in her new workplace, and internet messages spread information about the place where she is now employed. There are letters of complaint and finally the private institution where she works, decides to avoid public image problems and eventual problems with the government and makes her redundant. Emotionally exhausted, she does not know what do, and enters into a depressive state with a mixture of real and overvalued symptoms of persecution: it is impossible to distinguish, for her, true and imaginary danger. Countering the social media campaign is extremely complex. She first decides to restrict her movements to a minimum and stay at home except for essential trips outside. After some time, she moves to a different town. Shortly after, when she also receives death threats through phone messages in her new location, she takes the painful decision to go into exile.

This case is not fictitious. She is "H," a nurse working in Nicaragua. Many more cases of a similar nature are reported in other countries, especially concerning journalists[3] and human rights defenders, but quite often also normal citizens who are not even involved in political activities and are simply carrying out their jobs. H never saw her aggressor and never knew the true nature of the danger she faced. She was publicly accused, mocked and debased and was unable to identify the origin of the violence. There was effectively no need even to detain her, to produce severe psychological pain or suffering and to intimidate and coerce her.

A recent case study in Indonesia, Colombia, and Kenya (NDI, 2019) identified the widespread practice of hate speech, embarrassment and reputational risk, physical threats, and sexualised distortion of content targeting women activists, as dominant forms of threats and punishment.

Between December 2016 and March 2018, Amnesty International (AI) conducted qualitative and quantitative research on women's experiences of threats, violence, and abuse on Twitter. Their poll in 8 countries interviewed women and non-gender binary individuals (Dhrodia, 2018). The research highlighted the particular experiences of women of colour, women from ethnic or religious minorities, lesbian, bisexual or transgender women, non-binary individuals, and women with disabilities, to demonstrate the intersectional nature of threats, debasement, and abuse (Amnesty International, 2018). The research found that women, more often than men, were the target of threats of murder, rape, physical violence and graphic imagery via email, comment sections of newspapers and across all social media. As of 16 March 2018, Amnesty International had met with the Twitter CEO on three separate occasions to obtain a clear policy from the site, and, at the time of publishing the report, had not re-

3 https://www.elsalvador.com/eldiariodehoy/periodistas-instan-a-gobierno-no-ignorar-acoso-en-redes-sociales/625770/2019/

ceiving a satisfactory answer. There has been some progress since then[4].

On 27 January 2017, Ugandan human rights activist, Dr. Stella Nyanzi, wrote a post on Facebook in which she dubbed the Ugandan president 'a pair of buttocks' (Rukundo, 2018). The message was widely reproduced and as a consequence, she was then subjected to various forms of public internet threats by state agents that limited her activity. In spite of that, the threats culminated in her arrest on 7 April 2017. She was charged with cyber harassment and offensive communication contrary to sections 24 and 25 of the Ugandan Computer Misuse Act (CMA), which is vague legislation developed to restrict freedom of expression and political dissidence in the country. She was sentenced and jailed.

ICIT: Shame

Nelson Julio Alvarez, known as Nexy J. Show, a Cuban LGBTIQ activist and YouTuber, was detained by the Cuban Security Services, who seized his digital devices including his computer and mobile phone. During the weeks that followed, they replaced his identity on social networks for the purpose of public denigration[5]. Ezequiel Fuentes, another Cuban LGBTIQ cyber activist on Facebook was also the target of a widespread defamation campaign in which alleged members of, or collaborators with, the Ministry of the Interior publicly revealed private information including his relationships, as well as his health records[6]. Alvarez was targeted through identity theft and humiliation and Fuentes through defamation. Both were painfully forced to reduce their online presence.

In an interview, UK journalist Nosheen Iqbal, often the target of internet attacks, emphasised the role of "followers" in internet violence; an uncritical mass of people who are ready to denigrate a person and reproduce the attitude of very aggressive ideological opinion makers. After writing opinion pieces, Iqbal experienced systematically that after certain individuals made deeply offensive comments in the mass media, swaths of others followed in what seemed to be a well-orchestrated strategy (Mijatovic, 2018).

Threats, shame and post-truth environments

Freedom on the Net is an international database that collates and analyses situations of manipulation of news fora, opinion groups, harassment and online attacks on human rights defenders. Their reports include a long list of countries that infiltrate so-called *trolls*[7] in discussion forums to manipulate and direct their content. Venezuela, the Philippines and Turkey are relevant examples among 30 countries where governments were found to employ armies of "opinion shapers" to create hegemony for government-supported viewpoints, drive particular agendas, and counter government critics on social media (Freedom House, 2017). In Turkey, for instance, the report describes *AK Troller*, or *White Trolls*, a group pertaining to the ruling Justice and

4 https://blog.twitter.com/en_us/topics/company/2019/hatefulconductupdate.html

5 https://www.washingtonblade.com/2019/10/24/policia-detiene-al-yutuber-cubano-nexy-j-show/

6 https://adncuba.com/noticias-de-cuba-derechos-humanos/lgbtiq/ciberbullying-contra-comunidad-lgbtiq-cubana-homofobia.

7 On the Internet a 'troll' or 'hater' is a user who intentionally seeks to provoke, offend or impoverish the conversation within an online community, such as a blog, forum or social network profile. See also the discussion on *Corporate, political, and special-interest sponsored trolls* in https://en.wikipedia.org/wiki/Internet_troll

Development Party and which is government funded. Some 6,000 people have allegedly been recruited by the party to monitor and manipulate discussions, drive specific agendas, and counter government opponents on social media (Freedom House, 2017).

These organised groups create *fake news* that are accepted in an uncontested way by an often uncritical mass of the population (Lazer et al., 2018). Such widespread situations of creating *parallel worlds* have given rise to a new field of knowledge in social psychology and sociology: *post-truth environments* or a *post-truth society*. These are defined as contexts in which people are more likely to accept arguments based on emotions and beliefs rather than those based on facts (Bunce, 2019; Harsin & Harsin, 2018). Lies and falsehoods or manipulated statistics are easily accepted by public opinion in as much as they support the desired emotions. A person or an organisation can be the target of a post-truth emotional environment. Internet followers can, in the same way, react to emotional slogans in environments of political polarisation without further reflection.

On the peripheries of torture: controlling human beings through the net

Until this point, we have described elements of the psychological foundations of internet and communications ill-treatment or torture, with various examples. The internet is about empowering individuals by providing access to information. At the same time however, it is becoming more and more a place where both state and private companies alike gather personal information that can potentially be used for intimidation and control, including surveillance of movements, acts and opinions. This can be linked, as far as the individual is aware, to the production of emotional suffering or pain for the purposes suggested by the Convention against Torture. We will review some of these additional facets in the second part of the paper.

Surveillance and control of human right groups and political activists

The European Court of Human Rights recently published a Fact Sheet on Mass Surveillance[8] with case law from Germany, UK, Russia and Hungary among other countries (ECtHR, 2019). They were selected relevant cases that violated Article 8 (right to respect for private and family life, home and correspondence) of the European Convention, including the *Big Brother Watch and Others v. the United Kingdom* (nos. 58170/13, 62322/14 and 24960/15) after the revelations by Edward Snowden regarding programmes of surveillance and intelligence sharing between the USA and the United Kingdom. The case concerned three types of surveillance conducted by the Government Communications Headquarters, or GCHQ, Britain's signals-intelligence agency: (a) bulk interception of communications under the TEMPORA program; (b) intelligence sharing and receipt in collaboration with the PRISM and Upstream programs run by the National Security Agency (NSA) and (c) the obtaining of communications data from service providers. It was the first ruling against Britain's mass-surveillance programmes since Edward Snowden's 2013 revelations[9].

Russia is an example of a country where internet usage is under full control by the state and surveillance is widespread. All cryptographic systems except those licensed by the Federal Security Service of the Russian Federation (FSB) are forbidden. All internet provid-

8 https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

9 For a full discussion of the hearing see https://www.lawfareblog.com/summary-big-brother-watch-and-others-v-united-kingdom

ers must install a software named SORM that allows filtering and remote control of internet traffic[10]. A special unit of the Secret Services is devoted to surveillance and internet control (HRW, 2017). In September 2017, WikiLeaks released "Spy Files Russia," confirming how state entities had full access to detailed data on Russian internet and cellphone users by its citizens as part of SORM[11]. Amongst many examples, when the Crimean journalist Mykola Semena was detained and sentenced for crimes against the state, the Russian Secret Service had full control over his computer.[12]

The British organisation Privacy International maintains a database and updated information on the systems of surveillance and control of groups and activists in different countries of the world[13] including persons from the anti-torture movement. It also maintains a Surveillance Industry Index[14] with detailed information of hundreds of companies offering internet monitoring and surveillance services to governments, armies, military institutions, and private companies. Many of their activities are manifestly illegal and target the control of and threat to citizens, and especially political dissidents and human rights activists.

The United States Federal Bureau of Investigations (FBI) uses control and monitoring mass surveillance systems. A report by Privacy International (2018) has documented infiltration and troll activities in the Facebook anti-torture group Mass Action Against Police Brutality. Privacy International also revealed the existence of an FBI document mapping social networks of peaceful climate change activists which includes both names and other personal data[15].

A recently leaked document published in US newspapers showed the existence of a secret database shared by different US security agencies to track activists, lawyers and human rights defenders travelling to the Mexico-USA border to help migrants[16]. Furthermore, LookingGlass Cyber Solutions, a private company hired by US Homeland Security gathered personal information on the internet of around 600 persons who had participated in demonstrations against Trump's migrant family separation process in 2018[17], a US practice that is considered by some scholars as torture (Gray, 2019).

The Israel based company Cellebrite offers the Universal Forensic Extraction Device (UFED) designed to retrieve chat logs, texts, and other data from phones, in some cases bypassing PIN codes or passwords[18]. A recent report[19] showed, for instance, its use in extracting information from Mohammed al-Singace, a Bahraini political activist who was later detained and tortured in custody. Cellebrite offers, among other services to governments, the tracking of phone cells of asylum seekers to obtain information, through their GPS records, regarding which countries they have visited since leaving their countries of origin and challenge asylum claims as non-credible

10 https://en.wikipedia.org/wiki/SORM
11 https://wikileaks.org/spyfiles/russia/
12 https://www.bbg.gov/wp-content/media/2017/02/Mykola-Semena%E2%80%94Fact-Sheet-2017.03.16.pdf
13 www.privacyinternational.org
14 https://sii.transparencytoolkit.org/
15 https://www.theguardian.com/us-news/2018/dec/13/fbi-climate-change-protesters-iowa-files-monitoring-surveillance-
16 https://www.nbcsandiego.com/news/local/Source-Leaked-Documents-Show-the-US-Government-Tracking-Journalists-and-Advocates-Through-a-Secret-Database-506783231.html
17 https://theintercept.com/2019/04/29/family-separation-protests-surveillance/
18 https://www.cellebrite.com/en/product/
19 https://bahrainwatch.org/amanatech/en/investigations/cellebrite

based on this data. According to journalist research, many European countries, including Germany, the UK and Austria use Cellebrite services as evidence to deport migrants[20].

A well-known case of surveillance software usage is that of Pegasus[21], the programme that came to light when R3D, a Mexican human rights organisation protecting freedom of expression discovered its systematic use by the government to spy on journalists and activists who were later targeted, some of them suffering threats, defamation, kidnapping or torture (R3D, 2017). The software consists of malware that infects Apple iPhones through a WhatsApp message or a failed phone call. The attacker has access to everything in the victim's device: email, messaging services, camera, and microphone. The software is manufactured by the Israeli company, NSO Group. On its website[22] the company claims to sell the tool exclusively to governments on the condition that it is only used "to combat terrorists" and notes that the software has saved "thousands of lives." The software is sold also to private companies and contractors through reseller companies such as Hacking Team. According to R3D, the government is billed around 75,000 euros per successfully controlled telephone. A report by the *Red en Defensa de los Derechos Digitales* (Network for the Defense of Digital Rights) evidenced that the software was acquired by the Mexican Army in 2012 and by the office of the Attorney General (PGR) in 2014. An impressive series of studies show how the use of Pegasus has been an essential element in the murdering of journalists and for targeting politicians, lawyers and opponents in Mexico.[23]

A research center, Citizen Lab[24] based at the University of Toronto, produces regular reports and provides advice against such practices. It has detected the use of Pegasus in 45 countries and other similar software in almost all countries[25].

Social control of population

Although beyond the scope of this review, we would also at least mention the three most well- known methods of social control of the population amongst those of which civil society groups are aware.

- *International Mobile Subscriber Identity (IMSI) Catchers*. This is a device that connects to mobile phones in a particular area and can, among other things, provide the exact location of the user, build a network of all the numbers with which the person makes contact, as well as the successive contacts of those contacts; block or intercept data; access the content of calls, text messages and web sites visited or send intimidating anonymous messages to other mobile phones[26]. As a counter-response effort, there

20 https://www.wired.co.uk/article/europe-immigration-refugees-smartphone-metadata-deportations
21 https://en.wikipedia.org/wiki/Pegasus_(spyware)
22 https://www.nsogroup.com/
23 https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/
24 https://citizenlab.ca/
25 Hacking Team owns another malware, also allegedly to detect terrorists, that, according to an exhaustive report by Derechos Digitales is employed by almost all governments in Latin America to control political opponents, journalists and human right defenders (Perez de Acha, 2016). The report considers that such software has spread rapidly because secret services from governments in the region have cooperation programs and share both technologies and databases.
26 https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks

are different free mobile apps that allegedly detect IMSI catchers.

- *Facial recognition systems*. These capture detailed images of the participants in meetings or demonstrations with high-resolution cameras located in very distant places or inside drones. These are compared by the police with photographs of citizens and cross-referenced with databases to identify individuals of concern. Its use is being questioned by civil society organisations (Ruhrmann, 2019) and it seems there are plans for a European Union strict regulation[27]. In a counter-response effort, the Center for Human Rights Science at Carnegie Mellon University has developed a tool that can collate video recordings made with smartphones by demonstrators to produce an account of police brutality (Aronson, Cole, Hauptmann, Miller, & Samuels, 2018). Different governments have counter-reacted with legislation that forbids the use of smartphones during demonstrations and imposes severe fines if police are recorded, including confiscation of the phone[28].
- *Social media intelligence* - often shortened to SOCMINT - refers to the massive monitoring and gathering of information posted on social media platforms. These are software systems that are capable of downloading an entire website, forum or communications within a group, monitoring a citizen's social networks and accumulating evidence against them.

In June 2019, in Egypt, amid the most repressive period for decades, the government-linked El Watan newspaper published a leaked Interior Ministry tender document inviting software companies to contribute to the development of an open-source intelligence system called the "Social Networks Security Hazard Monitoring System." It would monitor Facebook, Twitter, WhatsApp and Viber in real-time for usage that might "*harm public security or incite terrorism*." It would also screen content for "*vocabulary which is contrary to law and public morality.*" According to Wikithawra[29], an independent monitoring group, at least 76 people have been detained so far this year in Egypt for offenses related to "online publishing."[30]

Such great interest in controlling users via the internet is not surprising. For certain authors, the so-called Arab Spring is an internet-based movement lead by a new young generation (Cole, 2014). Egypt, Tunisia and Libya were, amongst others, examples of countries where new technologies harnessed the internet to organise nationwide protests on designated days and to delegitimise the regime with videos of police torture and exposing government corruption[31]. The murder of Khaled Said in Alexandria, after he was beaten to death in public, by plain-clothes police officers, in front of witnesses, is a good example. Autopsy photographs of his badly battered face were circulated immediately on the internet, provoking both widespread demonstrations and vigils – many of which were organised and announced on Facebook and Twitter. The Facebook group "We are all Khalid Said" later became a hub for activists and a source of information for the population[32].

27 https://euobserver.com/science/145707
28 https://blog.witness.org/2015/07/film-the-police-not-in-spain/
29 https://wikithawra.wordpress.com/
30 https://www.csmonitor.com/World/Middle-East/2014/0630/Citing-terrorism-Egypt-to-step-up-surveillance-of-social-media
31 http://misrdigital.blogspirit.com/
32 There is there a complex double-sword: internet can help in the fight for freedom, but it is at cost of enormous risks for those involved. Egypt's 2011 uprising early demonstrations

Broadcasting torture to produce collective fear and terror

Occupy Paedophilia is the name given to groups of ultra-nationalist Russian neo-Nazi youths who have made a name for themselves by publishing videos in which they torture young members of the LGBTI community. The groups use targeted dating apps to organise meetings with individuals under the pretense of a "date," who are then filmed while being humiliated and beaten. At least in one case, the torture ended in death. In mid-2013, the first videos and photos began to appear on YouTube and the social network VK.com, a Russian equivalent to Facebook. The members use VK to create cells. At its highest peak, there were around 500 cells of 8 to 10 members, distributed in cities all around Russia. Although their stated goal is to locate paedophiles, the videos of the victims are of LGBTI teenagers or young adults, who are tortured and beaten, and during which their sexual orientation or gender identity is revealed to family, friends and their wider communities. For several years, the Russian state, which had enacted several laws against so-called "gay propaganda," did not act against them despite having their members identified and appearing in newspapers and TV, providing relative impunity for these acts (Wilkinson, 2014). It was also coincident with Russia's actions at the Human Rights Council in pushing for a wide margin of appreciation when dealing with "traditional values." A group that imitated Occupy Paedophilia was created in Barcelona in 2013. In December 2019, its members were convicted of a crime against moral integrity and disclosure of secrets with aggravating circumstances of superiority and homophobia, after they had orchestrated meetings with gay men through dating apps with pretenses of romance or sexual intentions. Instead, the group collectively ambushed their targets in order to humiliate them, record their actions and spread videos publicly. In 2018, Sudan's security services tried to undermine growing popular protests by apprehending a group of students in Darfur, torturing them brutally until some "admitted" to producing bombs to pursue violent intent in the name of militia groups in Darfur, and spreading false confession video-recordings on Facebook and state television (Carmichael & Pinnell, 2019). Contrary to what was expected, however, this attempt to create a post-truth situation lead to a popular reaction. Facebook comments disputing the validity of the confessions went viral and fuelled protests. Social media posts bearing the hashtag #WeAreAllDarfur were shared thousands of times (Carmichael & Pinnell, 2019).

Legal initiatives to prevent and act against ICIT

In July 2018, the United Nations Human Rights Council approved a resolution on *The promotion, protection and enjoyment of human rights on the Internet* through which it encouraged State Parties to legislate on how to protect freedom in the net while at the same responding to global threats[33]. Two years prior, in 2016, the European Union institutions succeeded in forcing internet giants Facebook, YouTube, Twitter, Microsoft, and more recently Instagram, to adopt internal Codes of Conduct[34].

were organized via a Facebook page. All the organizers were detained just three days later and all followers were tracked, and many of them detained or interrogated. Not being part of these groups means not having access to information on when and where actions would take place, but accessing them presented high risk for detention, interrogation and torture (Tufekci, 2014).

33 A/HRC/38/L.10/Rev.1.

34 https://ec.europa.eu/info/policies/justice-and-

These provide for various commitments, and require companies to implement clear and effective procedures for examining complaints regarding hate speech, so that access to such content can be withdrawn or disabled within 24 hours. According to the fourth evaluation of the application of this code in February 2019, its implementation had succeeded in eliminating 70% of content identified as being hate speech. Google has allegedly tried to control the manipulation of forums and the use of hate speech through Perspective[35], an app that detects such practices and which can also be used by social organisations. There are not many examples of case law. Quite noticeably, on 14 January 2020, in the case of Beizaras and Levickas v. Lithuania, the European Court of Human Rights ruled against the State on the basis of discrimination, violation of family and private life, and lack of access to effective remedies, for failure to properly act or investigate homophobic hate speech on Facebook against an LGTBI activist.

Forensic and legal considerations

We have described situations in which a state causes or does not prevent nor put a stop to the intentional infliction of severe psychological suffering of a citizen to achieve coercion, humiliation or punishment without the need to resort to physical violence. How this suffering is distinct from those of traditional torture is a largely unexplored field. Medical and psychological research must support legal efforts to regulate these complex and multifaceted situations.

Online ill-treatment and torture must be recognised and acknowledged. The revelations by Snowden and others of the widespread practice of surveillance of citizens led to no consequences for the authorities implicated other than scandal for and prosecution of the whistleblower. According to some scholars, paradoxically, competition for citizen surveillance has in fact increased (Richards, 2019). The letters to the governments of the United States, United Kingdom, Ecuador and Sweden by Special Rapporteur Nils Meltzer regarding Julian Assange in 2019, showing forensic evidence of torture, was a landmark document that opened a path for recognition of ICIT[36].

There is a delicate line between freedom of expression and hate conduct, and public harassment that needs legal clarification. International legislation related to ICIT should consider protection measures, removal of harmful content in internet, as well as forms of restoration, rehabilitation, satisfaction assurances of non-recurrence, combining measures that are symbolic, material, individual and collective.

There is also a need for international regulations that force internet intermediary companies to guarantee data security and privacy, regulate and control companies selling spyware and hardware and software aimed to infiltration, surveillance and massive control of population. Similar to support for the control of international trade of weapons potentially usable as torture devices, comparable legislation related to the trade of software and hardware of ICIT-capable devices is also necessary.

There is additionally a need for clear regulations on government access to private information, including cloud storage systems and infiltration of personal devices without a judicial order. Anonymity or encryption is a right and it should not be suppressed, controlled or

fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

35 https://www.perspectiveapi.com/#/home

36 https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24642

restricted by any state. Humanitarian organisations must also seek greater understanding of how data and metadata collected or generated by their programs for social, political or humanitarian purposes, can be accessed and used by other parties for social control (Pirlot de Corbion et al., 2018). Organisations working with survivors have an ethical duty through the do-no-harm principle to avoid involuntarily putting people at risk of internet and communications-based torture.

Finally, a complex challenge for the medical field is how to address the specific needs of rehabilitation of survivors of ICIT, combining, as with other situations, therapeutic work in individual and collective domains, with a special focus on symbolic elements.

In this issue

Megan Berthold, Peter Polatin, James Lavelle, Craig Higson-Smith, Frederick Streets, Caitrin Kelly and Richard Mollica develop a Complex Care Approach (CCA) for treatment of torture victims that integrates medical, psychological, psychosocial and existential elements from a holistic perspective, and apply it to an hypothetical paradigmatic case. Rouf Khawaja and collaborators present a series of 40 cases of male victims of sexual torture in India with severe urological sequelae in defining the concept of *parrilla torture* and showing the interplay between medical and psychological sequels. Carme Vivancos and Iñaki Rivera present data from an early analysis of the safeguards in the medical examination of people detained in Catalonia (Spain) in the framework of civic protests. The analysis serves as a reminder that the ethical principles of the Istanbul Protocol must be respected in all circumstances. Their data evidences a request for more thorough investigation by the Spanish authorities. Sexual conversion therapies are still common practice in many countries around the world as a recent IRCT report has shown. The Independent Forensic Expert Group has been working over the past two years on an analysis of these practices as a form of ill-treatment or torture. The reader will find a landmark document: the group's latest Statement with the conclusions and recommendations to the international legal and medical communities.

Johan Lansen, one of the great European figures of the 20th century in the work with torture survivors, from his own experience as a Holocaust survivor, passed away in November 2019. Torture Journal reprints, as a posthumous tribute, the article that he published in the Journal of Medical Ethics more than 15 years ago with personal reflections on the ethical dilemmas of working with perpetrators. This is a brief but extraordinary contribution that we are honoured to rescue.

We are living in times of a global crisis of unknown magnitude. The world has had much experience of wars in which humans have fought against each other. It is the first time however in the contemporary age in which the world defends itself from a common enemy, and when the element that should unite humanity, that difficult to define concept that we call the human condition, is globally challenged. From the Journal we are compiling initiatives or situations to provide perspectives on the current pandemic and the work with torture survivors. You can send us contributions (papers, reflections, reviews or news). In addition, continuing with the regular work of the journal throughout this year, three specific Special Sections are planned: Physiotherapy in the rehabilitation of torture victims, work with victims in contexts of active and continuous violence, and forced disappearance as a form of torture. The Calls for Papers can be found on the Journal's website. We look forward to your contributions.

References

Amnesty International. (2018). *#ToxicTwitter: Violence and abuse against women online*. https://www.amnestyusa.org/wp-content/uploads/2018/03/Toxic-Twitter.pdf

Anderson, C., & Carnegey, N. (2004). Violent evil and the General Agression Model. In A. G. Miller (Ed.), *The social psychology of good and evil*. Guilford. New York.

Aronson, J. D., Cole, M., Hauptmann, A., Miller, D., & Samuels, B. (2018). Reconstructing human rights violations using large eyewitness video collections: The case of euromaidan protester deaths. *Journal of Human Rights Practice*, *10*(1), 159–178. https://doi.org/10.1093/jhuman/huy005

Barrera, L., & Rodríguez, C. (2017). *La violencia en línea contra las mujeres en México. Informe para la Relatora sobre la Violencia contra las Mujeres MS. Dubravka Simonovic*. Internet Es Nuestra. www.Internetesnuestra.mx

Basak, R., Sural, S., Ganguly, N., & Ghosh, S. K. (2019). Online Public Shaming on Twitter: Detection, Analysis, and Mitigation. *IEEE Transactions on Computational Social Systems*, *6*(2), 208–220. https://doi.org/10.1109/TCSS.2019.2895734

Bunce, M. (2019). Humanitarian Communication in a Post-Truth World. *Journal of Humanitarian Affairs*, *1*(1), 49–55. https://doi.org/10.7227/jha.007

Carmichael, F., & Pinnell, O. (2019). How fake news from Sudan's regime backfired. *BBC News*, pp. 1–10.

Cole, J. (2014). *The New Arabs: How the Millennial Generation is Changing the Middle East*. Simon & Schuster.

Debord, G. (1995). The Society of the Spectacle. *Society*, p. 154. https://library.brown.edu/pdfs/1124975246668078.pdf

Dhrodia, A. (2018). Unsocial media: A toxic place for women. *IPPR Progressive Review*, *24*(4), 380–387. https://doi.org/10.1111/newe.12078

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, *59*(3), 551–570. https://doi.org/10.1093/bjc/azy068

ECHRT. (2019). *Mass surveillance* (Vol. 8). https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

Freedom House. (2017). *Manipulating Social Media to Undermine Democracy*. https://doi.org/10.1080/00224545.1975.9923293

Gleeson, H. (2014). *The prevalence and impact of bullying linked to social media on the mental heath and suicidal behaviour among young people*. Dublin. https://assets.gov.ie/25088/59fb1e4948fc43028f931a6c1e0c8790.pdf

Gonzales, A. L., & Hancock, J. T. (2011). Mirror, mirror on my Facebook wall: Effects of exposure to Facebook on self-esteem. *Cyberpsychology, Behavior, and Social Networking*, *14*(1–2), 79–83. https://doi.org/10.1089/cyber.2009.0411

Gray, G. (2019). Disappearing refugees inside the United States. *Torture Journal*, *29*(1), 144–146. https://doi.org/10.7146/torture.v29i1.113206

Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, *59*(3), 530–550. https://doi.org/10.1093/bjc/azy052

Harsin, J., & Harsin, J. (2018). Post-Truth and Critical Communication Studies. In *Oxford Research Encyclopedia of Communication*. https://doi.org/10.1093/acrefore/9780190228613.013.757

Hodalska, M. (2019). Cyberbullying, Fear and Silence: From Bystanders to Cyber-Samaritans. *Perils of the Web: Cyber Security and Internet Safety*, (May). https://doi.org/10.1163/9781848885011_004

Hopper, E., & Hidalgo, J. (2006). Invisible_Chains: Psychological coercion of human trafficking victims. *Intercultural Human Rights Law Review*, *1*, 185/209.

HRC. (2018). *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 - A/HRC/38/47*.

HRW. (2017). *Online and on All Fronts. Russia's assault on freedom of expression*. Human Rights Watch. https://www.hrw.org/sites/default/files/report_pdf/russiafoe0717_web_2.pdf

IGF. (2015). *Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women*. Internet Governance Forum.

John, A., Glendenning, A. C., Marchant, A., Montgomery, P., Stewart, A., Wood, S., … Hawton, K. (2018). Self-harm, suicidal behaviours, and cyberbullying in children and young people: Systematic review. *Journal of Medical Internet Research*, *20*(4). https://doi.org/10.2196/jmir.9044

Koenig, K. A. (2013). *The "Worst". A Closer Look at Cruel, Inhuman and Degrading Treatment*. University of California, Berkeley - School of Law; University of San Francisco. Doctoral Dissertation.

Lageson, S. E., & Maruna, S. (2018). Digital degradation: Stigma management in the internet age. *Punishment and Society*, *20*(1), 113–133.

https://doi.org/10.1177/1462474517737050

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., … Zittrain, J. L. (2018). The science of fake news. *Science*, *359*(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

Leary, M. R., & Tangney, J. P. (2012). *Handbook of Self and Identity*. Guilford Press.

Luban, D. (2009). Human Dignity, Humiliation, and Torture. *Kennedy Institute of Ethics Journal*, *19*, 211–230. https://doi.org/10.1353/ken.0.0292

Maier, A. (2011). Torture. How Denying Moral Standing Violates Human Dignity. In E. Kaufmann, P., Kuch, H., Neuhäuser, C., & Webster (Ed.), *Humiliation, Degradation, Dehumanization* (pp. 101–118). Springer Netherlands.

Manago, A. (2014). *Identity Development in the Digital Age: The Case of Social Networking Sites.* Oxford Handbooks On-line.

Mijatovic, D. (2018). *New Challenges to Freedom of Expression: Countering Online Abuse of Female Journalists*. https://www.osce.org/files/f/documents/c/3/220411.pdf

NDI. (2019). *Tweets That Chill : Analyzing Online Violence Against Women in Politics*. www.ndi.org/tweets-that-chill

Ortega, R., Elipe, P., Mora-Merchán, J. A., Genta, M. L., Brighi, A., Guarini, A., … Tippett, N. (2012). The Emotional Impact of Bullying and Cyberbullying on Victims: A European Cross-National Study. *Aggressive Behavior*, *38*(5), 342–356. https://doi.org/10.1002/ab.21440

Parry, J. T. (2003). What Is Torture, Are We Doing It, and What if We Are. *Pitt. Law Review*, *64*, 237–249.

Perez de Acha, G. (2016). *Hacking team malware para la vigilancia en América Latina*. Santiago de Chile.

Phillips, E. M. (2011). Pain, Suffering, and Humiliation: The Systemization of Violence in Kidnapping for Ransom. *Journal of Aggression, Maltreatment & Trauma*, *20*(8), 845–869. https://doi.org/10.1080/10926771.2011.626512

Pirlot de Corbion, A., Hosein, G., Nyst, C., Fisher, T., Gerathy, E., Callander, A., & Bouffet, T. (2018). *The Humanitarian Metadata Problem: 'Doing No Harm' in the Digital Era*. (October), 130. Privacy International. https://privacyinternational.org/sites/default/files/2018-12/The HumanitarianMetadata Problem - Doing No Harm in the Digital Era.pdf

Pollmann, A. (2011). *Humiliation, Degradation, Dehumanization* (P. Kaufmann, H. Kuch, C. Neuhaeuser, & E. Webster, Eds.). https://doi.org/10.1007/978-90-481-9661-6

Privacy International. (2018). *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*. (April), 173. https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29.pdf

R3D. (2017). *Gobierno espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en Mexico*. Mexico. https://r3d.mx/2017/06/19/gobierno-espia/

Richards, J. (2019). Intelligence gathering, issues of accountability, and Snowden. In *Terrorism and State Surveillance of Communications.* (pp. 19–37). Routledge.

Ruhrmann, H. (2019). *Facing the future. Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement.*

Rukundo, S. (2018). My President is a Pair of Buttocks': The limits of online freedom of expression in Uganda. *International Journal of Law and Information Technology*, *26*(3), 252–271. https://doi.org/10.1093/ijlit/eay009

Scarry, E. (1985). *The body in Pain*. Oxford University Press.

Serra, L. (2018). On-line gender based violence. *Pikara - Online Magazine.*, *2*(December), 227–249. Pikara Magazine. http://lab.pikaramagazine.com/wp-content/uploads/2019/06/VIOLENCIAS_EN.pdf

Sussman, D. (2006). Defining Torture. *Case Western Reserve Journal of International Law*, *37*, 225.

T-CY. (2018). *Mapping study on cyberviolence*. Council of Europe. www.coe.int/cybercrime

Tufekci, Z. (2014). Social Movements and Governments in the Digital Age: Evaluating a Complex Landscape. *Journal of International Affairs, 68*(1), 1–18. http://blogs.cuit.columbia.edu/jia/files/2014/12/xvii-18_Tufekci_Article.pdf

Van der Wilk, A. (2018). *Cyber violence and hate speech online against women* (PE 604.979). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

Wilkinson, C. (2014). Putting "Traditional Values" Into Practice: The Rise and Contestation of Anti-Homopropaganda Laws in Russia. *Journal of Human Rights*, *13*(3), 363–379. https://doi.org/10.1080/14754835.2014.919218

Zhao, S. (2005). The Digital Self: Through the Looking Glass of Telecopresent Others. *Symbolic Interaction*, *28*(3), 387–405. https://doi.org/10.1525/si.2005.28.3.387