Asian Journal of Criminology (2023) 18:61–74
https://doi.org/10.1007/s11417-023-09396-9

Cyber Victimisation, Restorative Justice and Victim-Offender Panels

Teresa Lancry A. S. Robalo[1] · **Razwana Begum Bt Abdul Rahim**[2]

Received: 11 October 2021 / Accepted: 2 February 2023 / Published online: 17 February 2023

Abstract
In recent years, individuals study and work from home with some degree of normality. Technology and the Internet have become an essential part of life. This increased reliance on technology and constant engagement with the online world has its negative repercussions. However, it has increased the number of offenders involved in cybercrimes. Considering the aftermath of cybercrimes and the need to address the impact of cybercrimes on victims, this paper reviews the existing mechanisms, such as legislation, international frameworks and conventions. The main purpose of this paper resides in the discussion of the possible use of restorative justice in supporting the needs of the victims. Taking into consideration the cross-border nature of many of these offences, other solutions have to be considered in order to give the victims a chance to be heard and to heal the wounds caused by the crime. This paper argues for the use of victim-offender panels, which are meetings between a group of cyber victims and a group of convicted cyber offenders, allowing victims to express the harm caused by the crime, to be healed and giving room for the offenders to feel remorse, lessening thus the likelihood of recidivism, under the umbrella of reintegrative shaming.

Keywords Cyber victims · Restorative justice · Victim offender panels · Victims' needs

Introduction

Using technology to commit crimes is not a new phenomenon. In 1834, hackers stole financial market information from the French Telegraph System (Herjavec, 2019). In 1988, the first cyberattack, known as the Morris Worm, resulted in massive 'clogging' of the Internet (Goel, 2020). With social media coming to life in the early 2000s, cybercrime erupted and it continues to rise. Ordinarily, cybercrime is associated with the use of technology, a medium used to commit real-world crime in cyberspace. Cybercrime continues to evolve

✉ Teresa Lancry A. S. Robalo
teresaso@um.edu.mo

[1] Faculty of Law, University of Macau, Avenida da Universidade, FLL, Room 2029, Taipa E32, Macau SAR, China

[2] School of Humanities and Behavioural Sciences, Singapore University of Social Sciences, 463 Clementi Road, Singapore 599494, Singapore

and harms a large population of individuals. Without victims coming forward to report, many cybercrimes and respective offenders escape from any form of repercussion.

According to an assessment report published by INTERPOL (2020), there is a significant shift by cybercriminals from targeting individuals and small businesses to crippling major corporations, governments and critical infrastructure. Cybercriminals are unscrupulous in using crisis to their advantage, utilising all structures in the commission of a crime. By increasing the fear factor, manipulating the nature of individuals and organisations and by introducing scarcity and temptations, cybercriminals are able to thrive and gain in many situations.

Considering the reliance on technology and the constant threats posed by cybercriminals, this article aims to contribute to a feasible solution to address cybercrimes. Its main argument relies on the fact that restorative justice has a role to play in cybercrimes as well, being able to place victims at the same level as offenders, or even putting the victims first (Correia, 2021). Even though restorative justice targets the victim, the offender and the community, which is particularly clear in the traditional models such as family group conferencing, circle sentencing and victim-offender mediation, literature and practice have highlighted other models also included under the restorative justice umbrella, which allow a victim to meet the offender of a similar crime. These models are particularly relevant when the offender has been killed or has committed suicide. This paper advocates that victim offender panels can be used in cases concerning cyber victims, not only because the victim has indeed the need to be healed from the experience caused by the crime, but also due to the difficulties posed by the possible cross border nature of these crimes.

Defining Cybercrime

Cybercrimes are crimes committed through Internet. They are just "a change in the *modus operandi* of conventional acts" (Arsawati et al., 2021, p. 219). Cybercrimes might be divided into two different groups encompassing both high and low-tech crimes. On the other hand, cybercrimes might be generally understood as any criminal activity undertaken in cyberspace, as well as any offline crime that makes use of the Internet (for instance, stalking or defamation); but it might also be specifically defined as criminal behaviour that targets the machine itself (such as invading digital information through remote access to a computer) (Venâncio, 2011).

Low-tech crimes do not require any special technological knowledge by the offender. Since Internet democratisation, anyone who has access to it has a tool in his/her hands that allows him/her to immediately move from the offline world to an online scene, thus having a new and handily accessible arena to commit several crimes from defamation to stalking, from identity theft to any kind of fraud, from bullying to the encouragement of suicide, among many others. To do so, no one needs to have special knowledge in informatics, a mobile phone with Internet access is sufficient.

However, high tech crimes are commonly committed by hackers, individuals who have more knowledge on the Internet, cybersecurity and informatics issues than regular people (Venâncio, 2011). They are able to access from anywhere any unprotected device connected to the Internet and have enough skills to control, access and save the information or even affect it in order to get a ransom, as happened in The Netherlands where a click on advertising websites immediately downloaded malware into Internet users' devices. After its installation, the concerned devices immediately became inaccessible. Users then got

messages on the computer screens informing them that they had committed a crime and had to pay a 100 euros fine in order to regain access to their devices. It affected 65,000 people who believed in such scareware (Wagen & Pieters, 2020).

In 2020–2021, millions of people all around the world had to stay home for weeks, even months, due to the pandemic caused by COVID-19. Thanks to Internet democratisation, it was possible to overcome isolation by allowing online classes and work. Online platforms became particularly famous all around the world, allowing dozens of people to gain access to online meetings. Among them, naked uninvited hackers were found accessing online classes, a case known as "Zoombombing".[1]

In April 2020, UNODC released a report enhancing the connection between quarantine measures and cybercrime. For instance, children became much more vulnerable to sexual abuse; adults were more exposed to possible risks, such as online fraud and sextorsion as well as phishing; and senior adults became perfect targets to download ransomware links about the virus (UNODC, 2020). Consequently, there are currently a potentially higher number of victims of cybercrimes who need protection and, particularly, to have their lives restored.

Generally speaking, any criminal activity that involves a computer, networked device or a network can be classified as cybercrime. Cybercrime can be divided into two categories, cyber-dependent crimes and cyber-enabled crimes. The hacking and infecting of computers leads to cyber-dependent crimes. Cyber-enabled crimes adopt information technology as a resource, with the result that traditional forms of criminal activities, such as fraud, bullying and stalking, occur in cyberspace (Furnell et al., 2015). Cybercrime may damage or disable computers or devices directly. Cybercrimes can also spread malware, illegal information, images or materials.

Cybercriminals might be driven by the will to harm the victim's good reputation, which is particularly clear in defamation or data theft but also in identity theft, for instance (Jaishankar, 2020).

Cybercrimes are a consequence of the development of the society. On another hand, their *locus delicti* is not in the real world, but rather in the virtual world. Thus, usually the victim and the offender do not have any physical contact and there is a high likelihood that the offender is located in another legal system. This causes problems related to international and national legislation, as well as with extradition (Arsawati et al., 2021).

Challenges and Safeguards

The proliferation and dependency on technology raises extensive challenges. Cybercrime leading to monetary loss is just one aspect of the challenge. The other significant issue that requires greater attention is the impact of cybercrime on victims, especially those who are vulnerable and emotionally traumatised by online bullying, fraudulent love connections or fake news. A report on Southeast Asia and its dissonance with online child pornography highlights the dire situation of images of children permanently remaining in cyberspace, causing much trauma to the children and their loved ones (Davy, 2017).

[1] E.g. https://www.berkeleyside.com/2020/04/08/berkeley-unified-suspends-online-classes-after-naked-zoombomber-enters-session.

The pandemic changed the work model, forcing non-frontline employees to work from home using technology to be online and available. This created a large space in which cybercriminals could thrust their unlawful activities. To mitigate this challenge, companies, organisations and governments adopted ad hoc systems and arrangements aiming at containing cyberattacks while maintaining business continuity.

This paper provides a suggestion in the form of restorative justice to deal with the consequences of cybercrime. This does not offer a solution to the complex problem of cybercrime or cybersecurity. Instead, it invokes the different stakeholders to reconsider and review their strategies from restorative lenses, incorporating the principles and values of restorative justice in determining the response to some cybercrimes.

Consequences of Cyber Victimisation and Victims' Needs

Cyber victims have no longer to be in the same physical space than their offenders, which allows the latter to attack anyone, located anywhere, several people at once, or even organisations or States (Jaishankar, 2020). Cyber victims are the targets of any offense committed through Internet—not only offenses such as cyberbullying or cyberstalking. We agree with Jaishankar (2020) and with his typology of cyber victimisation. However, for the sake of this study, we will focus on cybercrimes involving adult victims, such as identity theft, credit card fraud victims, victims of content theft (e.g. content published in blogs) or romance fraud victims, stressing out how restorative justice can play an important role in such cases.

Based on Dutch cyber victim reports, Leukfeldt et al. (2018) considered that there are no major differences between the consequences of offline and online crimes from the standpoint of the victims. Online crime victims mainly report feelings such as fear, guilt, helplessness, shame or anger. However, depending on the concrete online crime, these consequences might have a major or minor impact, either psychologically or emotionally. For instance, these authors mentioned sexting, cyberstalking, fraud or identity theft to demonstrate that their impact on victims might be significant, which is particularly clear with respect to sexting when victims' nude pictures are circulating online. Victims feel guilty, ashamed, depressed and afraid that such pictures or videos will continue emerging online without any time limit, having a significant impact on their reputation, socially or even at work. They might become paranoiac and their main concern is not only the offender's conviction but also that the police help them to withdraw such pictures or videos from the web as soon as possible. One shall also note that if these materials were collected online, victims might not know the offender's real identity or even his/her location, which increases their feelings of constant fear (Leukfeldt et al., 2018). These victims often experience secondary victimisation as police are usually not prepared to deal with such cases and society as a whole may blame them for having sent or having allowed someone else to take nude pictures or videos. On the other hand, there are cases of revenge porn victims who committed suicide due to their inability to deal with the exposure of their privacy on the web without their will and control.[2]

[2] E.g. https://www.smh.com.au/lifestyle/revenge-porn-victim-driven-to-suicide-in-italy-as-courts-order-her-to-pay-costs-over-bid-to-remove-video-20160919-grjfxc.html.

With respect to cyberstalking, authors have highlighted that it either started offline and continued online by a known offender or it started online. In terms of consequences, it might cause feelings of fear and lack of safety, anywhere and anytime. With respect to fraud, victims experience financial consequences and sometimes only want the case to be reported to the bank. Victims also feel it is hard to prove that they are not the person who shows as them in identity theft cases. They feel insecure and not trusted by the authorities or even guilty for something they have not done (Leukfeldt et al., 2018).

In sum, cyber victims need to be recognised as such by the authorities and they need to have more training on online crimes so they are able to take action as soon as possible (which is particularly clear in revenge porn cases). Instead of sometimes having their complaints rejected, the victims need to tell their stories and be properly heard as in the case of any offline victim (Leukfeldt et al., 2018). Their emotions and feelings need to be addressed and they need to be involved in the judicial proceedings and be protected against secondary and repeated victimisation.

International Legal Framework and Case Law on Cybercrime

Given that cybercrime might be committed by anyone located in any country through any device connected to the Internet, international law plays a dramatic role in terms of prevention and standardisation of national rules, not only about proper measures to be taken when facing cybercrime but also on matters related to the extradition of the offender to another jurisdiction. However, in order to increase the world's conscience to this phenomena—which is no longer new—and to eradicate the feeling of impunity, it is vital to understand how the international community as well as the international Courts, such as the European Court for Human Rights, are dealing with this reality. It aims at giving a general picture on how law addresses the issue and what is still to be done on behalf of the cyber victims' needs, leading to the conclusion that restorative justice is an extra tool aiming at filling in a gap that cannot be addressed by law itself.

UNODC highlights that "the rules of evidence and criminal procedure are not standardised between countries. Similar rules of evidence and criminal proceeding are needed for cybercrime because this form of crime transcends borders and impacts digital devices and systems anywhere in the world with an Internet connection".[3]

Therefore, it is important to highlight the existence of several conventions, whether multilateral or bilateral, on cybercrime issues because such crimes assume a natural cross-border nature and demand a coordinated and supranational response. States are entirely free to consider that they have jurisdiction over such crimes, namely if the offender or the victim is their national or even due to the universality principle. However, this does not collide with the need and effective existence of international conventions in order to find uniform standards to deal with these crimes, which might be committed anywhere in the world against anyone, no matter the victim's age, gender or nationality.

The Council of Europe Convention on Cybercrime (2001) includes a set of measures to be taken at the national level in terms of substantive and procedural law, even though it focusses on high-tech cybercrimes. It also adds norms related to State jurisdiction, thus

[3] https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

increasing the likelihood of criminal prosecution as well as international cooperation and extradition.

In contrast, the African Union Convention on Cyber Security and Personal Data Protection (2014) starts with a set of provisions on obligation law and deals with cybercriminality in its Chapter III, giving a special importance to national cyber security. It also states several rules on international cooperation in terms of harmonisation, mutual legal assistance, exchange of information and means of cooperation. This Convention encompasses a broader set of cybercriminal offences, including high-tech and low-tech offences. For instance, in accordance with its article 30, States shall adapt their legislation in order to include certain crimes, namely against property, when committed through information and communication technologies or to consider such means as aggravating circumstances. The need for an effective punishment is highlighted in article 31, paragraph 1.

The agreement on cooperation among the State members of the Commonwealth of Independent States in combating offences relating to computer information (2001) focuses on high-tech cybercrimes (article 3), and the Arab Convention on Combating Information Technology Offences (2010) brings a set of comprehensive substantive and procedural norms about high-tech cybercrimes as well as rules on extradition and mutual assistance.

The existence of international conventions on the matter shows that States' international organisations at the regional level are aiming to set rules on cybercrime, namely on high-tech cybercrime, and are willing to find harmonisation between national legal systems and the promotion of effective punishment for these transnational crimes.

Indeed, the punishment of the offender is one of the main needs of the victim after a cyberattack. However, since interpersonal crimes are not dealt with in such instruments, victims are not extensively protected and their needs are not taken into account, at least at a primary level. It is undeniable that victims' needs should also be taken into account in high-tech cybercrimes since their data might be stolen, and bank account information, private data or the computer system might be affected by any malware or scareware. However, one may also consider victims of any traditional offline crime if committed through information and communication technologies since the impact of such crimes on victims' lives is also considerable and their needs should also be taken into account. For instance, how will the State with jurisdiction over the case deal with the need for financial compensation? How will the police in any member State deal with any cyber victim? What steps should be taken in order to withdraw sensitive data from the web as soon as possible?

In practical terms, it is relevant to recall Directive 2012/29/EU of the European Parliament and of the Council (2012) which aims to ensure "that victims of crime receive appropriate information, support and protection and are able to participate in criminal proceedings". Crime victims are considered such irrespective of the offline or online nature of the offence (Paunovic, 2018). The Directive encompasses several measures that are aimed at preventing secondary victimisation as well as reinforcing respectful treatment and recognition by anyone who deals with a crime victim, including police officers. It also deals with financial compensation and restorative justice processes. As an effective international instrument with respect to the protection of victims, it is also a masterpiece related to victims' needs after the victimisation experience.

International case law is also relevant in this regard. For instance, the European Court of Human Rights has already decided on cases related to cyber victims, such as the case of K.U. v. Finland (02/03/2009). The Court ruled that Finland violated article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom as to the right to respect for private life. This case concerned a 12-year-old boy whose picture was used by someone without his consent on a website aimed at attracting paedophiles and on which

the boy's name and accurate contacts were added. He was indeed contacted by email by a man willing to meet him. His father placed a complaint and the server provider was asked to inform the authorities about the offender's IP. However, the server provider refused to do so, arguing that it was bound by the confidentiality of the telecommunications in accordance with the law.

The police asked the Court to oblige the service provider to provide such information, but the District Court argued that the offence—malicious misrepresentation—was not one that allowed the disclosure of the information. The Court of Appeal refused to grant leave to appeal.

Consequently, the victim of this crime was unable to identify the person who used the victim's personal data and picture and placed it in an advertisement webpage without his consent. The European Court of Human Rights considered that article 8 of the Convention not only protects private life in general, including physical and moral integrity, but also obliges the States to take positive measures in order to ensure effective protection of these rights. Furthermore, this act is a criminal offence with respect to a minor, placing him in a particularly dangerous position vis-a-vis the paedophiles.

The Court added that, apart from having to protect the aforementioned rights, the State has to provide a remedy for their violation, "enabling the actual offender to be identified and brought to justice (…)" which was certainly denied by the national Courts' decisions. In addition, freedom of expression and confidentiality of communications are not absolute values and might be restricted based on the need to protect other fundamental rights. Thus, it was the task of the legislature to create a concrete framework under which these rights could be properly protected, allowing the offender to be identified and brought to justice.

This case enhances the need for State parties to provide full protection to cyber victims, especially because they have the ability to reduce certain fundamental rights, such as freedom of expression and confidentiality of communications, when other fundamental rights are affected by a criminal behaviour, including the right of physical and moral integrity affected by some online offences. States should definitively facilitate the identification of online crime suspects, as well as offline suspects, bringing them to justice and offering the victim the feeling of protection and security as well as deterring other potential online offenders from acting in the same way.

Restorative Justice and Cybercrimes

As argued by Braithwaite (1999), restorative justice is a process that aims to bring together those who were affected by a crime, such as the offender, the victim and the community. It aims at restoring social peace, allowing both victim and offender to overcome the criminal experience. On the one hand, the victim needs to tell his/her story, to be heard, to express the consequences caused by the crime, apart from financial and other needs; on the other hand, and following Braithwaite's (1989) theory of reintegrative shaming, the shame caused to the offender by being exposed to his/her acts and the extension of their consequences is an important tool to help him/her reintegrate into the society, and not to repeat the behaviour onwards.

Allowing victims to voice out what they have gone through, during and after the offense, as well as letting offenders understand the harm caused and express remorse for their acts, is fundamental in restorative justice (Brewer et al., 2019).

Restorative justice is a concept that looks at the outcome of a transgression or a crime taking the victim, the offender and the community into consideration (Wenzel et al., 2008). It is a traditional relationship-based justice model that focuses on the victim as well as on the offender; however, restorative justice is more victim oriented than traditional criminal proceedings (Brewer et al., 2019). The objective of restorative justice is to find ways to repair the harm caused by a certain offence. The concept may appear to be novel, but the principles and values of restorative justice are not contemporary. Restorative justice is usually referred as being based on community-based justice models implemented by indigenous communities globally, either in Canada, North America, Australia or New Zealand, among others. However, there are scholars who are highlighting that such a statement is just a myth, a convenient myth, which repetition has led to an "uncontested truth statement" (Tauri, 2016, p. 54).

The concept promotes "voluntary, community-based response to criminal behaviour" by bringing "together the victim, the offender, and the community, in an effort to address the harm caused by the criminal behaviour" (Latimer et al., 2005, p. 131).

The development of restorative justice in the last few decades has been remarkable (Sherman & Strang, 2007). Initially introduced for juvenile offenders in the early 1970s, the concept has evolved to support different conflicts in various situations (Peachey, 1989). Restorative justice is emerging within the business world (Goodstein & Aquino, 2010). As argued by Qafisheh (2012), the values, principles and characteristics of the concept of restorative justice are still evolving.

There are several reasons why this concept is popular. First, the focus is on victims. Victims of crime suffer the most but they are seldom part of the criminal justice system. By incorporating restorative justice, the victims are at the centre of an offence or a transgression (Weatherburn & Macadam, 2013). Second, restorative justice reduces the rate of reoffending (Bonta et al., 1998; Klingele, 2019). Restorative justice requires involvement of all stakeholders, including the offender and the larger community. The participation of the offender in the resolution process increases his or her understanding of the offence and its impact on the victim. Community involvement strengthens an offender's willingness to change. The change occurs either through shaming of the behaviour or via support and encouragement from the community members (Braithwaite, 1989).

Restorative justice focuses on relationships between the different stakeholders, including the victim, the perpetrator and the community. According to Zehr and Mika (1998), crime is fundamentally a violation between people that affects their interpersonal relationships, and such violations create obligations and liabilities. The obligation and liability is not just contained between the parties involved. Crime control is a community responsibility and victims are placed at the centre of the resolution process. There is a need to involve all stakeholders, including the larger community. Restorative justice can heal and put right the wrongs. To achieve this outcome, it is necessary to focus on the principles of restorative justice that are rooted in values such as responsibility, respect, restoration and reparation (Abdul Rahim, 2017; Tracy, 1998).

The principles and values of restorative justice can be easily assessed and reviewed in the context of the criminal justice system. For instance, when using restorative justice in the administration of young offenders, there are higher victim–offender satisfaction rates, lower rates of reoffending and higher rates of offenders paying reparation through the adoption of restorative justice practices such as victim–offender mediation (Latimer et al., 2005; Levi et al., 2015). In the context of cybercrime, crime control and resolution is not simple. Furthermore, the application of restorative justice in this area is speculative (Brewer et al., 2019; Button et al., 2015; Levi et al., 2015). However, there is some adaption of restorative

justice in the area of cybercrime, notably in the context of young offenders and getting them to understand the impact of their actions on victims (Levi et al., 2015).

Restorative justice models traditionally refer to victim–offender mediation, family group conferencing and circle sentencing (Brewer et al., 2019). However, other conferences also aim at restoring the victim, the offender and the communities, such as victim offender panels that bring together victims and offenders of similar crimes but not the exact victim and his/her offender (Van Ness & Strong, 2015).

Beyond the traditional criminal sphere, restorative justice is also a relevant tool in school and labour environments. Values such as responsibility, reintegration, restoration and respect underpin restorative justice practices (Dignan, 2005; Marshall, 1999). Apart from responsibility, reintegration is often made possible with some form of restoration. Even though in most criminal matters, it may not be possible to completely restore the situation for the victim, it is important to consider restoration. The value of restoration is made possible through the healing process that occurs between parties involved in transgressions. For instance, restoration for both the victim and the offender is made possible by allowing them the opportunity to discuss and voice their grievances. This value provides an opportunity for the offender to pay back to the victim in ways that may make the victim feel safe and protected as a member of a community. This is one of the key differences between restorative justice and traditional forms of justice. Restoration of a sense of justice happens with renewed value consensus (Okimoto et al., 2009). An apology can be the easiest form of restoration, and in the context of cybercrime, it is equally important to acknowledge the harm done to the victim, even if it is not possible to completely restore or repair the impact of the action on the victim.

Relationship building takes place by including the transgressor in the conflict resolution process. Involving the offender increases the level of acceptance and reintegration of the offender back to an organisation or into a community. The influence of community and peer groups is observed in how cyber offenders are engaged and held responsible for their action initiated and supported. This article suggests that similar forms of support can lead to crime prevention and reduction of recidivism.

Restorative justice and its practices are often viewed as an addendum to the formal criminal justice system, which provides an alternative crime response and is rarely visible in the formal administration of justice. However, restorative justice models might be either alternative or cumulative to the criminal justice (Brewer et al., 2019). This paper advocates that restorative justice in the context of cybercrime is complementary to the criminal justice and, thus, should not be viewed as a replacement of the existing justice model.

As mentioned previously, traditional practices of restorative justice include victim offender mediation, sentencing circles and family group conferencing (Wong & Gavrielides, 2019; Lauwaert & Aertsen, 2015). These practices as illustrated by Brewer et al. (2019) are relevant in addressing cybercrime and its aftermath. Cybercrime is complex with its unidentified victims and perpetrators, but it causes considerable harm, especially to vulnerable victims. This paper, however, suggests adopting restorative justice principles and values in designing a systemic framework to deter or prevent cybercrime.

For restorative justice to be applied in a cybercrime, it is necessary to first identify all stakeholders. The challenge here is not just about gathering the needs of all stakeholders, it is about creating a mutual desire to prevent and stop cybercriminals.

Fundamentally, restorative justice is concerned with harm reparation, not punishment. This frame of reference alters both the starting point of the process as well as the roles of participants in the procedure. Ultimately, the objective is restoration for all affected parties

(Braithwaite, 1989, 2000). Victims either do not feel confident in reporting cybercrimes to the police, which is particularly clear in what concerns to female victims (Jaishankar, 2020), or the criminal justice itself is based on a retributive model and not in a restorative one, focusing in the offender and in punishment (Correia, 2021). Restorative justice solutions take the harm into account, as well as how it shall be repaired (Correia, 2021). Cyber victims consider such mechanisms as positive; in addition, they will have the chance to meet the offender, who was hidden behind a computer or some other electronic device (Button et al., 2015) as well as to understand why they have been selected (Brewer et al., 2019). However, there are no empirical studies up-to-date to understand if restorative justice brings positive outcomes in what concerns to cybercrime prevention (Brewer et al., 2019).

Nevertheless, traditional restorative justice models may pose several difficulties with respect to cybercriminality. Even when victims place a complaint, it is not easy to find the offender. Thus, it is uncommon to bring these offenders to justice (Button et al., 2015). Even when they are found, proper restorative justice solutions will always depend on the consent of both of the involved parties. In addition, cybercrime involves an extra challenge due to its cross-border nature. Not only is it not an easy task to identify the offender, but the offender might be a national of a State without criminal regulations on the matter or which opposes his/her extradition for criminal purposes. If one considers the physical travel of the offender just for restorative justice purposes, additional costs will be added. Such costs might be properly cut off if we move to the digital world, from which everything indeed started, and suggest, for instance, victim offender mediation through online meeting platforms. Even though it could be a proper remedy to several constraints caused by the cross-border nature of several cybercrimes, one may ask if the lack of a physical encounter between the victim and the offender would not distort the nature of restorative justice.

On the other hand, restorative justice mechanisms vary depending on the type of online crime that was indeed committed. For instance, in cases of cyberbullying and attending to the average age of both the offender and the victim, family group conferencing seems appropriate (Duncan, 2016; Langos & Sarre, 2015), which in turn is not appropriate for online fraud, such as romantic or monetary fraud, a malware or a scareware. Thus, even though restorative justice mechanisms are seen with sympathy by cyber victims, several aspects should be taken into account in this regard.

Victim-Offender Panels and Cybercrime

A possible solution to the abovementioned problems could be found in victim offender panels (VOP) with online offenders, allowing them to meet the victims of similar crimes in the offline world. It would give the victims a chance to express the consequences of the crimes on their lives, to tell their stories and to be heard; and it would allow offenders to understand the extension of their acts and thus be a proper tool to reduce recidivism.

Impact panels are indeed a possible way to reach restorative justice objectives without following a traditional model, such as victim-offender mediation (VOM). The offender might have died, might not be caught, or the victim might not want to see "his/her" offender, among many other reasons preventing such a meeting to occur (Van Ness & Strong, 2015). In these panels, a group of victims will not meet "their" own offenders, but rather a group of offenders who have committed similar crimes. Research shows that victims are satisfied with this model, which allows them to tell their stories, to be

heard, and to feel less anger; on another hand, offenders understand the extension of the harm caused and research shows an effective impact on offenders' attitudes, as well in the likelihood of recidivism (Van Ness & Strong, 2015).

Victim-offender panels might take several forms. For example, in England, there is a program that allows a group of victims of burglary to meet a group of young offenders who have committed similar crimes and both victims and offenders will have the chance to discuss (Van Ness & Strong, 2015). Another popular expression of a victim-offender panel is the Victim Impact Panel, which is organised in the USA by the Mothers Against Drunk Driving (MADD). There is one single meeting where the victims speak and no interaction between victims and offenders are allowed (Thompson & Joyce, 2022; Van Ness & Strong, 2015).

Victim-offender panels in general, and Victim Impact Panels in particular, are compatible with restorative justice and reintegrative shaming (Thompson & Joyce, 2022). The positive outcomes of these encounters rely on the chance given to the victim to heal his/her wounds and to be empowered, having an active voice in the aftermath of the crime, as well as giving the offenders who committed similar crimes the opportunity to understand the extent of their acts and their impact on real people with the aim of modifying their actions (Staiger, 2010). Thompson and Joyce (2022) have developed a research aiming at understanding if Victim Impact Panels have effects on reducing the likelihood of recidivism of driving under the influence of alcohol. Their research has shown that "attending a Victim Impact Panel reduced the odds of a subsequent DUI by 49% and 77% at 5 and 8 years, respectively" (Thompson & Joyce, 2022, p. 9). Some authors also advocate Victim Impact Panels for terrorism cases, particularly because the offender might be deceased but the victim's needs still need to be addressed (Staiger, 2010).

We advocate that victim-offender panels are perfectly compatible with online offences. Not necessarily because the offender has died, but due to the cross-border nature of these offences which creates several difficulties in identifying the offender or in extraditing him/her to another jurisdiction. If this is an issue due to national protective legislation, it is even less feasible if one considers an international trip just to attend a restorative justice conference. In practical terms, if this or any other similar solution is not accepted, the victim will be abandoned not only by the system itself because the offender will hardly be brought to justice, increasing the feeling of impunity in the society, but because no other complimentary solutions will be applicable.

Victim-offender panels can be organised offline, as well as online through competent mediators/facilitators trained to do so and with the collaboration of national authorities. Nevertheless, we recognise that it might be easily feasible in the offline world. At which moment? In our opinion, it makes particular sense while the offender is serving time in prison (Ness, 2007). The reason is clear: we are arguing that victim-offender panels are suitable for cybercrimes, and the main characteristic of such conferences resides in the fact that victims will meet offenders other than their own. In order to have an offender, and no longer a defendant, criminal justice has to have decided on the case and convicted the offender. Consequently, such victim offender panels should be organised while the offender is serving time in prison, upon the consent of both victim and offender. We consider that these panels are a useful way to address some of the cyber victims' needs, such as the need to voice their experiences and consequences, and to regain power over the situation and thereby proceed with their lives. On another hand, offenders also need to be given a voice, in order to place victims and offenders at the same level and aiming at reaching the remorse and behaviour change onwards.

As mentioned above, for the sake of this study, we have in mind cybercrimes involving adult victims. And the reason is that the particular needs and fragilities of minor victims, together with the fact that they need to be accompanied by their parents or other guardians, or the special approach that sensitive matters deserve, require particular studies on how (and if) restorative justice can be used in this situation. On another hand, the authors focus on some crimes such as identity theft, credit card fraud victims, victims of content theft or romance fraud victims, for instance, because it will be either hard to find the offender, or he/she might be in another country, or the victim really does not want to meet his/her offender but rather someone else who has committed a similar crime (which seems more obvious in romance fraud victims). Therefore, victim offender panels are a way to address both the victims' needs and the offenders who have been found guilty of similar crimes, under the guidance of trained mediators/facilitators. On one hand, victims will feel empowered after having had the chance to tell their stories and offenders will have the chance to understand the harm caused to the victims by their behaviour, lessening the chance of future repetition of the same acts.

However, we also argue that not a single solution is sufficient to cope with the consequences of cybercrimes on victims. The judicial process keeps on being fundamental to protect fundamental values, such as the rights of those that are affected by the crime, not to mention the need for compensation/restitution. Authorities also need to receive special training regarding victims' needs and how to deal with them in a respectful way, avoiding secondary and repeated victimisation. Only a holistic approach will meet cyber victims' needs, thereby improving their lives and the community as a whole.

Conclusion

Online crimes are an increasing reality. Cyber victim has several needs, some of which are different than that of offline victims, such as, for instance, the withdrawal of nude pictures and videos from the online scene. Nevertheless, they also need to be recognised and secondary victimisation should be prevented. They need to get financial compensation, but they also might need to meet the offender, to tell their stories, to be heard and to heal the wounds generated by crime. International law and case law are clear in regard to the need to protect them. Restorative justice plays an important role here as a complementary tool to traditional criminal justice. Even though there are different models under the restorative justice umbrella, not all of them seem to be applicable to all cybercrimes. Due to cross-border victimisation constraints, this paper advocates the use of victim-offender panels, namely in a post-sentencing stage.

Funding University of Macau.

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Ethical Approval Nothing to add.

Informed Consent Not applicable.

Conflict of Interest The authors declare no competing interests.

References

Abdul Rahim, R.B. (2017). The potential of restorative justice in strengthening corporate governance framework. *Internet Journal of Restorative Justice,* 5 Year Celebration Special Issue, ISSN (online), 2056–2985.

Arsawati, I., Darma, I., & Antari, P. (2021). A criminological outlook of cyber crimes in sexual violence against children in Indonesian laws. *International Journal of Criminology and Sociology, 10*, 219–223.

Bonta, J., Wallace-Capretta, S., & Rooney, J. (1998). *Restorative justice: An evaluation of the restorative justice project*. (User Report 1998 - 05). Solicitor General Canada.

Braithwaite, J. (1989). *Crime, shame and reintegration*. Cambridge University Press.

Braithwaite, J. (1999). Restorative justice: Assessing optimistic and pessimistic accounts. *Crime and Justice, 25*, 1–127.

Braithwaite, J. (2002). *Restorative justice and responsive regulation*. Oxford University Press.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Restorative justice. In M. Gill (Ed.), *Cybercrime prevention. Crime prevention and security management* (pp. 109–122). Palgrave Pivot. https://doi.org/10.1007/978-3-030-31069-1_8

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2015). Online fraud victims in England and Wales: Victims' views on sentencing and the opportunity for restorative justice? *The Howard Journal, 54*(2), 193–211.

Correia, S. (2021). Cybercrime victims: Victim policy through a vulnerability lens. Electronic copy available at: https://ssrn.com/abstract=3897927.

Davy, D. (2017). Regional overview: Sexual exploitation of children in Southeast Asia. Bangkok: *End Child Prostitution, Child Pornography, and the Trafficking of Children for Sexual Purposes (ECPAT) International*, 35–36.

Dignan, J. (2005). *Understanding victims and restorative justice*. Open University Press.

Duncan, S. H. (2016). Cyberbullying and restorative justice. Navarro, R., Yubero, S. & Larrañaga, E. (Eds.), *Cyberbullying Across the Globe* (pp. 239–257). Springer International Publishing

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes. *Computer Fraud & Security, 2015,* 5–12.

Goel, S. (2020). National cyber security strategy and the emergence of strong digital borders. *Connections, 19*(1), 73–86.

Goodstein, J., & Aquino, K. (2010). And restorative justice for all: Redemption, forgiveness, and reintegration in organizations. *Journal of Organizational Behavior, 31*, 624–628.

Herjavec, R. (2019). Cybersecurity CEO: The history of cybercrime, from 1834 to present. Cybercrime Magazine. Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present

INTERPOL (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Jaishankar, K. (2020). Cyber victimology: A new sub-discipline of the twenty-first century victimology. In An international perspective on contemporary developments in victimology, 3–19. Springer.

Klingele, C. (2019). Measuring Change: From Rates of Recidivism to Markers of Desistance. *The Journal of Criminal Law and Criminology, 109*(4), 769–817.

Langos, C., & Sarre, R. (2015). Responding to cyberbullying: The case for family conferencing. *Deakin Law Review, 20*(2), 299–319.

Latimer, J., Dowden, C., & Muise, D. (2005). The effectiveness of restorative justice practices: A meta-analysis. *The Prison Journal, 85*, 127–144.

Lauwaert, K., & Aertsen, I. (Eds.). (2015). *Desistance and restorative justice: Mechanisms for desisting from crime within restorative justice practices*. European Forum for Restorative Justice.

Leukfeldt, R., Notté, R. & Malsch, M. (2018). Online crime victimization. Needs, consequences and responsibilities following victimization through cybercrime and digital crime. Summary. Available at https://english.wodc.nl/binaries/2839_Summary_tcm29-368217.pdf

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2015). *The implications of economic cybercrime for policing*. City of London Corporation.

Marshall, T. (1999). *Restorative justice: An overview*. Home Office Research Development and Statistics Directorate.

Okimoto, T. G., Wenzel, M., & Feather, N. T. (2009). Beyond retribution: Conceptualizing restorative justice and exploring its determinants. *Social Justice Research, 22*(1), 156–180.

Paunovic, N. (2018). Cyberbullying of children: Challenges of victim support. *Temida, 21*(2), 249–268.

Peachey, D. (1989). The Kitchener experiment. In M. Wright & B. Galaway (Eds.), *Mediation and criminal justice: Victims, offenders and community* (pp. 14–26). Sage Publications.
Qafisheh, M. M. (2012). Restorative justice in the Islamic penal law: A contribution to the global system. *International Journal of Criminal Justice Sciences, 7*(1), 487–507.
Sherman, L. W., & Strang, H. (2007). *Restorative justice: The evidence*. Smith Institute.
Staiger, I. (2010). Restorative justice and victims of terrorism. In R. Letschert, I. Staiger, & A. Pemberton (Eds.), *Assisting victims of terrorism* (pp. 267–337). Springer.
Tauri, J. (2016). Indigenous peoples and the globalization of restorative justice. *Social Justice, 43*(3), 46–67.
Thompson, K., & Joyce, S. (2022). Do victim impact panels have sustained effects on DUI recidivism? *Laws, 11*, 28. https://doi.org/10.3390/laws11020028
Tracy, C. (1998). Associate editor's editorial: The promises and perils of restorative justice. *International Journal of Offender Therapy & Comparative Criminology, 42*, 275–277.
UNODC (2020). Cybercrime and COVID19: Risks and responses. https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf
Van Ness, D. V. (2007). Prisons and restorative justice. In G. Johnstone & D. W. Van Ness (Eds.), *Handbook of Restorative Justice* (pp. 312–324). Willan Publishing.
Van Ness, D., & Strong, K. (2015). *Restoring justice: An introduction to restorative justice* (5th ed.). Routledge.
Venâncio, P. D. (2011). *Lei do cibercrime anotada e comentada*. Coimbra Editora.
Wagen van der, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480–497.
Weatherburn, D., & Macadam, M. (2013). A review of restorative justice responses to offending. *Evidence Base, 2013*(1), 1–20.
Wenzel, M., Okimoto, T. G., Feather, N. T., & Platow, M. J. (2008). Retributive and restorative justice. *Law and Human Behavior, 32*(5), 375–389.
Wong, D.S.W and Gavrielides, T. (2019). *Restorative justice in educational settings and policies: Bridging the East and West*. RJ4All Publications.
Zehr, H., & Mika, H. (1998). Fundamental concepts of restorative justice. *Contemporary Justice Review, 1*, 47–55.