Personal data and personal safety: re-examining the limits of public data in the context of doxing

Batuhan Kukul*

Key points

- Doxing is a form of cyber harassment that involves the malicious collection and dissemination of personal information, often resulting in threats of violence, loss of employment, and other negative consequences.
- As social media usage has increased, people have become more willing to share personal information. This trend has made it easier for cyberbullies to collect and share either public or private personal information and publish it online to cause harm. However, people should be able to use the Internet without fear of physical or psychological harm.
- This article provides various definitions of doxing and explains the methods that are commonly used in doxing.
- This article examines the criminal offenses of different countries, including the USA, EU, and Turkey, to explore the existing legal framework and identify potential remedies for punishing and preventing the disclosure of personal information with malicious intent.
- Furthermore, it illustrates how data privacy law, can be used to combat doxing under the purpose limitation principle.
- Finally, the article emphasizes the importance of the legal values that are threatened by doxing and proposes a perspective for future doxing legislation.

Introduction

Andrew Anglin, the editor of a magazine that sympathizes with neo-Nazis, published photos, phone number, e-mail, and social media profiles of Tanya Gresh, a wedding organizer for the Jewish community, on the largest neo-Nazi website.[1] After that, Gresh's phone kept ringing, she received countless death threats and anti-Semitic messages. Furthermore, Gresh was forced to delete all of her social media accounts. She had to hire security guards to be stationed outside her house. But the threats did not stop. Following that, Gresh began to experience panic attacks, and her physical health deteriorated. In her own words, 'What they did to me wasn't harassment, it was terrorism, they took away everything in my life'. Gresh sued Andrew Anglin for violating her privacy and causing mental and emotional distress under the Anti-Intimidation Act. Anglin was sentenced to pay $14 million as compensation.[2] Gresh said that if there was an anti-doxing law, maybe this attack would never have happened to her.[3] This case highlights how exposing sensitive information about individuals on the Internet with malicious intent can bring the dangers of the online platform into the physical world.[4]

*Attorney at law, Research Fellow, LLM Candidate, Bahcesehir University, Istanbul, Turkey. Email: batuhan.kukul@bahcesehir.edu.tr

1 Alexander Lindvall, 'Political Hacktivism: Doxing & the First Amendment' (2019) 53 Creighton Law Review 1.

2 Mallory Simon and Sara Sidner, 'Neo-Nazi website founder ordered to pay $14M for troll storm.' *CNN* (8 August 2019) <https://edition.cnn.com/2019/08/08/us/montana-jewish-woman-federal-judgment-neo-nazi-soh/index.html> accessed 30 May 2022.

3 Luke O'Brien, 'The Making of an American Nazi', *The Atlantic* (Boston, December 2017), <https://www.theatlantic.com/magazine/archive/2017/12/the-making-of-an-american-nazi/544119/> accessed 15 May 2022.

4 Stine Eckert and Jade Metzger-Riftkin, 'Doxxing, Privacy and Gendered Harassment. The Shock and Normalization of Veillance Cultures' (2022) 68 M&K Medien & Kommunikationswissenschaft 273, 287.

Many countries have enacted criminal offenses and published legal guidelines to combat cyber harassment. Recently, Hong Kong's legislature enacted an amendment to privacy law that directly addresses the public release of information identifying an individual or organization.[5] On the other hand, the European Union (EU) has implemented its General Data Protection Regulation (GDPR)[6] since May 2018 to give users more control over their personal data online, including the right to be forgotten, which can be used by targets of doxing to have personal information removed from search engine results. In addition to cybercrime regulations in its Criminal Code, Germany has also implemented the Facebook Act in 2018, which imposes heavy fines on social media platforms that fail to remove hate speech, fake news, and illegal content within 24 hours of its posting.[7]

The Crown Prosecution Service, an independent organization that prosecutes criminal cases that have been investigated by the police and other investigative organizations in the UK, released detailed guidelines for prosecutors on what constitutes criminal online harassment.[8] Turkey has also enacted an anti-stalking statute. In the USA, there are currently few legal remedies for the victims of doxing. While these approaches may be implemented to address particular cases, they may not provide complete protection against doxing in practice. Doxing is a multifaceted issue that includes a wide range of methods and technologies and requires a comprehensive approach.

This article will begin by providing a definition of the term 'doxing' and an overview of the methods utilized by cyberbullies. Subsequently, the criminal framework of Turkey, the USA, and the EU region will be analysed to highlight the advantages and limitations of these frameworks in combatting doxing, together with those of some selected other countries. While individuals may choose to publish personal information about themselves on the Internet, the question remains whether this always justifies the collection and distribution of publicly available personal information with malicious intent. This article aims to emphasize the importance of protecting personal data used in doxing, even if that data are publicly accessible. To support this argument, the purpose limitation principle in data privacy law will be examined. Since doxing not only violates privacy but also jeopardizes many legal values, this article will propose a new perspective for future doxing legislation.

Definition of doxing

There is no legal definition of doxing. The term 'dox' is derived from the slang 'dropping dox', an old revenge tactic that emerged in 1990s hacker culture.[9] Scholars have provided various definitions of doxing.

According to Professor Mary Anne Frank, the definition of doxing is the public release of an individual's private, sensitive, or personal information, such as home address, email address, phone number, social security number, and employer contact info, family member's contact information, photos of the victim's children and the school they attend.[10] Sarah Jeong thinks that doxing means the publication of a physical residential address, or information protected by law.[11] Gabriella Coleman defines doxing as the leaking of private information such as social security numbers, home addresses, or personal photos. In addition, she does not limit doxing to legally protected information.[12] On the other hand, The Oxford References Dictionary describes doxing as an online practice of exposing personal information about others which had previously been kept private.[13] The European Institute for Gender Equality defines 'doxing' as the online gathering and dissemination of private information on the Internet in order to publicly expose and shame the person being targeted.[14] According to McIntyre, doxing is a type of harassment that occurs when someone publishes private information (usually through a deep Internet search or hacking) such as a phone number, home address, or social security number

5 Office of the Privacy Commissioner for Personal Data, Personal Data Privacy Amendment Bill 2021 (8 October 2021) <https://www.pcpd.org.hk/english/doxxing/index.html> accessed 23 January 2023.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

7 German Law Archive, Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG) (1 October 2017) <https://germanlawarchive.iuscomp.org/?p=1245> accessed 23 January 2023.

8 The Crown Prosecution Service, Social Media and Other Electronic Communications Legal Guidance Cyber and Online Crime (19 December 2022) <https://www.cps.gov.uk/legal-guidance/social-media-and-other-electronic-communications> accessed 23 January 2023.

9 Younes Karimi and others, 'Automated Detection of Doxing on Twitter' (2022) 6 Association for Computing Machinery 3.

10 Julia M MacAllister, 'The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information' (2018) 85 Fordham Law Review 2451, 2456.

11 Sarah Jones, 'Stop Diluting the Definition of Dox' <https://sarahjeong.net/2015/07/08/stop-diluting-the-definition-of-dox/> accessed 18 May 2022.

12 Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy* (Verso 2014) London and New York 418.

13 Oxford, 'A Dictionary of Social Media' <https://www.oxfordreference.com/view/10.1093/acref/9780191803093.001.0001/acref9780191803093-e-405> accessed 20 May 2022.

14 European Institute for Gender Equality, <https://eige.europa.eu/thesaurus/terms/1654> accessed 20 May 2022.

and publishes that information online without permission.[15]

Extortion, coercion, and harassment can all be made easier with the release of this information.[16] Doxing can take place in different methods and for numerous purposes. According to MacAlister, doxers typically have three different intentions. She distinguishes three types of doxing based on the actor's intent: punching down doxing (ie, doxing for purely malicious purposes), doxing for political purposes, and the use of doxing as a tool for internal regulation by members of anonymous online communities (ie, unmasking).[17]

Douglas, on the other hand, distinguishes three types of doxing based on the type of information revealed and the motivation behind it: deanonymizing, targeting, and delegitimizing.[18] Deanonymization provides detailed information that relates an individual's anonymous or pseudonymous identity to their true identity. Targeting reveals information about an individual that can be used to locate them physically, such as their home address or workplace. Delegitimising exposes potentially embarrassing or humiliating information about an individual.

Types of doxing

Sometimes doxers deliberately carry out attacks against a specific group of people in society.[19] Celebrities are one of the groups that have been consistently exposed to doxing.[20] Celebrities are frequently featured in news articles. However, doxing is not one of the typical magazine articles. In this form of doxing, someone discloses sensitive information about celebrities such as credit card information, e-mail addresses, social security numbers, or phone numbers to cause harm or loss of reputation. Celebrities such as Paris Hilton, Kim Kardashian, Joe Biden, Hillary Clinton, and Donald Trump have all been affected by doxing.[21]

Doxers sometimes associate the wrong people with unrelated events.[22] As a result of this kind of 'faulty' doxing, innocent people face problems such as loss of reputation, loss of employment, harassment, physical harm, or death. For instance, back in 2013, Sunil Tripathi, an innocent student, was wrongly identified as the perpetrator of the Boston Marathon bombing by vigilantes on Reddit.[23] Following that, Tripathi disappeared, and after a while, his dead body was found in the sea near a park, and his death was declared a suicide.[24]

Cyberbullies sometimes use doxing as a tool for taking revenge on their enemies. This situation is called Revenge Doxing.[25] To give an illustration, Curt Schilling, a former Major League Baseball pitcher, wanted to take revenge on those who made sexually abusive comments about his daughter on Twitter in March 2015.[26] Schilling tracked down the people behind the fake Twitter accounts and found out their real names. After that, he exposed some of their sensitive information on the Internet. Following this, another cyberbully was fired from his job and another was expelled from his college because of the incident.[27] Other unknown cyberbullies were afraid of being exposed for doxing and apologized to Schilling and his daughter on social media.

Swatting Doxing happens when cyberbullies report their victims to the police for the purpose of joking or sometimes to harass or cause harm to them.[28]

15 Victoria McIntyre, 'Do(x) You Really Want to Hurt Me?: Adapting IIED as a Solution to Doxing by Reshaping Intent' (2016) 19 Tulane Journal of Technology, and Intellectual Property 111, 113.

16 David M Douglas, 'Doxing as Audience Vigilantism against Hate Speech' (2020) Open Book Publishers 259, 260.

17 MacAllister (n 10) 2457.

18 David Douglas, 'Doxing: A Conceptual Analysis' (2016) 18 Ethics and Information Technology 199, 203.

19 On the other hand, it should be emphasized that women are more likely to have certain types of private information posted online and to receive higher amounts of unwanted, vitriolic messages. See Amanda Lenhart and Kathryn Zickuhr, 'Online Harassment, Digital Abuse, and Cyberstalking in America' (2016) CIPHR <https://www.datasociety.net/pubs/oh/Online_Harassment_2016.pdf> accessed 22 May 2022.

20 Back in 2010, hacker Christopher Chaney collected personal email information on celebrities such as Scarlett Johansson, Mila Kunis, and Christina Aguilera, including nude photos and private emails and published them online. *See* Julia Moyer, 'Doxing: Dangers and Defenses' (2016) Tuffts University 8.

21 Gautam Khoiwal, 'Legal analysis of doxxing', *Eduindex News* (3 July 2021) <https://eduindex.org/2021/07/03/legal-analysis-of-doxxing/> accessed 22 May 2022.

22 Vanya Verma, 'Legal analysis of doxxing' (*Pleaders*, 1 July 2021) <https://blog.ipleaders.in/legal-analysis-doxxing/> accessed 25 May 2022.

23 Traci G Lee, 'The real story of Sunil Tripathi, the Boston bomber who wasn't', *NBC News* (22 June 2015) <https://www.nbcnews.com/news/asian-america/wrongly-accused-boston-bombing-sunil-tripathys-story-now-being-told-n373141> accessed 21 May 2022.

24 Kaspersky, 'What is doxing' <https://www.kaspersky.com.tr/resource-center/definitions/what-is-doxing> accessed 22 May 2022.

25 Medha Mehta, 'What is doxxing? 5 Examples of doxxing and how to prevent it' (Infosec Insights, 26 March 2020) <https://sectigostore.com/blog/what-is-doxxing-5-examples-of-doxxing-and-how-to-prevent-it/> accessed 25 May 2022.

26 Scott Stump, 'Baseball legend Curt Schilling defends his daughter against vulgar Twitter replies', *Today* (10 April 2015) <https://www.today.com/parents/mlb-legend-curt-schilling-defends-his-daughter-against-vulgar-twitter-t14036> accessed 25 May 2022.

27 Cam Smith, 'College student suspended for tweets he wrote about Curt Schilling's teenage daughter', *USA Today High School Sports* (2 March 2015) <https://usatodayhss.com/2015/curt-schilling-lashes-out-at-twitter-trolls-threatening-lewd-acts-with-hs-senior-daughter> accessed 25 May 2022.

28 Jason Fagone, 'The Serial Swatter', *New York Times* (29 November 2015) <http://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=2> accessed 26 May 2022.

Additionally, they notify the police the victim's name and address. Then the police dispatched a SWAT team to the victim's home.[29] For example, back in 2015, three months after introducing the swatting bill in Congress, Katherine Clark noticed flashlights in her home. Police officers with rifles were blocking off her street. Officers informed her that they have received an anonymous phone call stating that there is an active shooter at Clark's house.[30] Swatting doxing is the most terrifying type of doxing because they use real weapons and equipment against the victim.[31]

Although swatting is often done for entertainment purposes, it can also be used as a tool for committing severe crimes such as homicide. In crime doxing, perpetrators release personal information about their competitors on the Internet and encourage others to harm them. The motivation may be personal revenge or expressing disagreement or hostility towards a particular cause, religion, activity, or race.[32]

In late 2004, Cecilia Barnes ended a lengthy relationship. Her ex-boyfriend retaliated by creating a fake Yahoo account using Barnes' name and posting her nude photos, alleged sexual fantasies, personal and business contact information without her consent. He used the account to join Yahoo chat rooms and send photos and messages to other users, resulting in Barnes receiving harassing emails, calls, and attempted visits to her home. Despite repeated requests to Yahoo to deactivate the fake account, her requests were denied.[33] Barnes' complaint against Yahoo, which appeared to allege two causes of action under Oregon law, was declined by the court.[34]

National approaches to doxing and their limitations

Today, doxing is a serious problem as the line between online and offline life has become blurred due to the widespread use of smartphones and social media platforms. As a result, to effectively combat doxing, it is necessary to establish laws that explicitly prohibit such behavior. In this context, the following section will examine various approaches that can be used to combat doxing, based on the laws of different countries.

The US Communication Decency Act 1996, section 230

To date, there is currently no specific legislation in the USA that prohibits doxing.[35] Scholars argue that doxing is directly related to the First Amendment,[36] and that a balance must be established between privacy rights and freedom of expression.[37] Doxers often defend themselves by claiming they are simply exercising their right to free speech.[38] While the First Amendment forbids Congress from enacting legislation that restricts freedom of expression, Supreme Court decisions have determined that freedom of expression does not have absolute protection.[39] In the case of a serious threat (The True Threat), freedom of expression may be restricted under the circumstances of a substantial case.[40] The totality of the circumstances will be considered by the court to decide whether the speech is a true threat or not. From this perspective, it can be argued that doxing may be considered a True Threat and thus can be prohibited under the True Threat exception to the First Amendment.

29 Tyler Barriss was involved in a dispute between two other players, Casey Viner and Shane Gaskill, while playing an online video game in December 2017. According to NBC News, Viner challenged Barriss to defeat Gaskill, and Gaskill accepted the challenge, revealing his previous address. It is now occupied by the family of a man named Andrew Finch. Barriss tricked Gaskill by calling the cops a prank. Barriss pretended to be himself and told the cops that he killed his father and took the rest of his family hostage. Finch was killed by one of the police officers who intervened after he was searched from the outside. For the fake call, Barriss was sentenced to 20 years in prison. *See* Micheal Brice-Saddler and others, 'Rankster sentenced to 20 years for fake 911 call that led police to kill an innocent man', *The Washington Post* (29 March 2019) <https://www.washingtonpost.com/nation/2019/03/29/prankster-sentenced-years-fake-call-that-led-police-kill-an-innocent-man/> accessed 26 May 2022.

30 Ann Friedman, 'Katherine Clark is taking on the trolls', *Elle* (13 July 2016) <https://www.elle.com/culture/tech/a37728/katherine-clark-harassment-abuse-legislation/> accessed 28 May 2022.

31 McIntyre (n15) 113.

32 In the late '90s and early 2000s, Neal Horsley, an anti-abortion activist, compiled the names, photos, and addresses of abortion providers and posted them on the Nuremberg Files website. He has labeled this list as a 'hit list'. Eight doctors from the Nuremberg list have been killed so far. The website praised the victims of such murders and urged pro-life activists to continue assassinating doctors on the kill list. *See* Meave Duggan, 'Online Harassment' (Pew Research Center, 22 October 2014) <https://www.pewresearch.org/internet/2014/10/22/online-harassment/> accessed 26 May 2022.

33 *See Barnes v Yahoo!, Inc* 570 F.3d 1096, 1098–99 (9th Cir 2009) (This case describes the doxing of Cecilia Barnes in conjunction with the publication of pornographic photos taken without her consent).

34 *See Barnes v Yahoo, ibid.*

35 Lisa Bei Li, 'Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting' (2018) 70 Federal Communication Law Journal 318, 322.

36 Patricia R Recupero, 'New Technologies, New Problems, New Laws' (2016) 44 The Journal of the American Academy of Psychiatry and the Law 322, 323.

37 MacAllister (n 10) 2462. *See* also Henrik Sigurdh, 'Recontextualising Doxing: Discursive Practices Before and After the U.S. Capitol Riots' (Master thesis, Umeå University 2021) 21.

38 Gina Vaynshteyn, 'Doctor of pharmacy Savannah sparks is here to blast vaccine deniers and racists on TikTok' (Distractify, 2 May 2021) <https://www.distractify.com/p/savannah-sparks-pharmacist-tiktok> accessed 30 May 2022; *See* Lindvall (n 1) 2.

39 *Giboney v Empire Storage & Ice Co* 336 US 490, 498 (1949); *See Commonwealth v Johnson*, 21 NE3d 937, 946–47 (Mass 2014).

40 *Virginia v Black*, 538 US 343, 359–60 (2003).

The Communication Decency Act (CDA), broadly prohibits child pornography and other obscene and inappropriate content that is accessible to children on the Internet, with exceptions in terms of criminal law and intellectual property law.[41] The CDA states that:

> no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[42]

For example, YouTube cannot be treated as the publisher of videos that users upload, according to the CDA. In other words, online intermediaries that host or republish speech are shielded from a variety of laws that could otherwise hold them legally liable for what others say and do. Thus, service providers or users of interactive computer services cannot be held responsible for the content shared by users or others who share the content of third parties. Furthermore, these actors are not required to investigate whether the content is illegal or not if they are not acting as content providers. As a result of this liability shield, in the Gamergate case, Twitter could not be held responsible under the CDA for users who dox Brianna Wu.[43]

The US Interstate Communications Statute, section 875(c)

The Interstate Communications Statute, section 875(c) specifically criminalizes the Internet transmission of any communication containing any threat to kidnap any person or any threat to injure the person of another.[44] Importantly, 875(c) states that the threatened party does not need to actually receive the threat.[45] Federal prosecutors could use section 875(c) to prosecute actors who dox in combination with administering threats. Indeed, this statute could apply to the Gamergate actors who harassed, threatened, and doxed Wu and others. However, 875(c) only penalizes explicit threats to kidnap or injure a person. In many cases of doxing, an actor may never explicitly threaten to kidnap or injure the victim. Doxing may just include the target's name and a few contact information, but the victim may still be terrified. In other words, the perpetrator can cause harm or terrorize the victim without threatening, kidnapping, or injuring them. On the other hand, doxing occurs not only with the purpose of threatening or injuring but also for other reasons such as loss of reputation.

The US Interstate Stalking Statute, section 2261A(2)

The Interstate Stalking Statute (ISS) prohibits the use of any interactive computer service in a 'course of conduct' that places a person in a reasonable fear of death or serious bodily injury or causes substantial emotional distress to a person.[46] The ISS requires intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person.[47] Section 2261A requires a 'course of conduct' for any offense. 'Course of conduct' is defined as 'a pattern of conduct composed of two or more acts.[48] The ISS has the potential to be a useful tool for preventing some forms of doxing, but it is insufficient because of its 'course of conduct' requirement. Various threads were exposed with 'someone initiating the abuse and others piling on'. If each actor was only responsible for one or two particular acts, no single person could be held liable because of the 'course of conduct' requirement under section 2261A.[49] On the other hand, despite the fact that over three million people are reportedly stalked online each year, the ISS results in the prosecution of only about three of those individuals.[50]

Consequently, it can be stated that these statutes do not provide effective and consistent remedy because their terms are underinclusive and they are rarely enforced in combating doxing.

Article 123(A) of the Turkish Panel Code: stalking statute

Stalking has been added to the 5237 numbered Turkish Penal Code[51] as a crime following the law amendment on 27 May 2022. Article 123(A) states that 'any person

41 47 US Code 223(a).

42 47 US Code 230(c)(1).

43 On the evening of 10 October 2014, a Twitter user known as 'Death to Brianna' began tweeting rape and death threats against Brianna Wu, the head of development at independent game studio Giant Spacekat. The user's picture, which appeared next to each tweet, was of Wu and her husband. The user went into graphic detail about his plans to rape, murder, and mutilate Wu, as well as kill her children and torture her husband. The user was harassed four minutes after it began and wrote: 'Guess what bitch? I now know where you live. You and Frank live at [home address redacted]. *See* MacAllister (n 10) 2452.

44 18 US Code 875 (c).

45 *United States v Kistler*, 558 F Supp 2d 655, 656 n.2 (WD Va 2008).

46 18 US Code 2261A.

47 18 US Code 2261A (2).

48 *United States v Bell*, 303 F.3d 1187, 1192 (9th Cir 2002), 18 USC 1514(d)(1), <https://www.law.cornell.edu/uscode/text/18/1514#d_1> accessed 1 April 2022.

49 Danielle Keats Citron, 'Hate Crimes in Cyberspace' (2014) 27 Harvard University Press 136.

50 Lindvall (1) 10.

51 1 June 2005 dated 5237 numbered Turkish Penal Code. The purpose of the Penal Code is to protect individual rights and freedoms, public order and security, the rule of law, peace in the community, public health and the environment, and to prevent the commission of offences. In order to achieve this objective of criminal responsibility, specific criminal offences, penalties and security measures are regulated under this statute.

who persistently causes a serious disturbance to another person or is worried about the safety of themselves or one of their relatives by physically following them or attempting to contact them by using any communication tools or information systems, or by third parties, shall be punished with a term of imprisonment from six months to two years'.[52]

Although Article 123(A) comes close to covering some instances of doxing, it is not sufficient to provide a completely effective solution against doxing for two reasons. First, Article 123(A) requires conduct such as 'following' or 'attempting to contact' the victim either physically or online. However, doxers can jeopardize their victims without physically following them or making any direct or indirect contact with them. Secondly, whether Article 123(A) can be used to prosecute malicious doxing depends on whether the dox constitutes a 'course of conduct'. The title of Article 123(A) emphasizes that acts such as 'following' or 'attempting to contact' should continue persistently. Nevertheless, perpetrators can cause harm to their targets without persistently following or attempting to contact them.

Article 123 of the Turkish panel code: disrupting people's peacefulness and tranquility

Article 123 of the Turkish Panel Code states that 'any person who with the intent of disturbing people 's peace and tranquility by persistently making phone calls, making noise or doing any other unlawful act for the same purpose, shall be punished with a term of imprisonment from three months to one year upon the complaint of the victim.'[53]

Article 123 does not limit the conduct of disturbing people. Accordingly, any unlawful act that means to disturb people's peace and tranquility will violate Article 123. From this point, doxing could be considered an unlawful act; therefore, Article 123 may be used for substantial doxing cases. However, Article 123 also does not provide a sufficient safeguard against doxing for two reasons.

First of all, under Article 123 it is insufficient to make a few phone calls or make noise for a short period of time. Article 123 requires course of conduct as a provision of the crime. Thus, the unlawful act must be continued persistently. As mentioned above, in most doxing cases, the perpetrator can terrify the victim with just a few acts.

Furthermore, under Article 123, the perpetrator's intention must be 'disrupting people's peace and tranquility'. Nonetheless, doxing may be committed with the intent of killing, harming, or humiliating people. As a result, the specific intent, and course of conduct requirements of Article 123 limit the liability for doxers.

Consequently, although there are offenses that can be applied against specific doxing cases, it can be stated that there is no effective law that directly punishes doxing in the Turkish Penal Code.

The UK section 1 of the MCA 1988

The UK Crown Prosecution Service's (CPS) cybercrime guidance lists a number of possible offenses that could be related to cybercrimes, including making a death threat,[54] disclosing private sexual images without consent,[55] harassing or stalking someone,[56] publishing material which may lead to the identification of a complaint of a sexual offense,[57] and taking, distributing, possessing, or publishing indecent images of children. These offenses might be committed as a result of doxing; however, these offenses do not directly prohibit doxing and could only apply in specific and narrow situations. The CPS highlights two acts, the Malicious Communications Act 1988 (MCA 1988) and the Protection from Harassment Act 1997 (PHA 1997) for combating cybercrimes.

Section 1 of the MCA makes it an offense for a person, with the intention of causing distress or anxiety, to send certain items to another person that convey an indecent or grossly offensive message or are themselves of an indecent or grossly offensive nature or convey a threat or information that is false and known or believed to be false by the sender. The England and Wales High Court has interpreted 'grossly offensive' as follows:

> The [offender] intended his message be grossly offensive to those to whom it related; or that he was aware at the time of sending that it might be taken to be so by a reasonable member of the public who read or saw it.[58]

In another decision, the Administrative Court held that:

> For the offence s.127(1)(a) to have been committed the sender must have intended or been aware that the message was not simply offensive but grossly offensive. The fact that

52 Panel Code 2005, 123/A.
53 Panel Code 2005, 123.
54 Section 16 Offences against the Person Act 1861.
55 Section 33 Criminal Justice and Courts Act 2015.
56 Sections 2, 2A, 4 or 4A Protection from Harassment Act 1997.
57 Section 5 Sexual Offences (Amendment) Act 1992.
58 *DPP v Kingsley Smith* [2017] EWHC 359, CO/6265/2016 <https://www.bailii.org/ew/cases/EWHC/Admin/2017/359.html> accessed 28 January 2023.

the message was in bad taste, even shockingly bad taste, was not enough.[59]

Therefore, for an offender to commit this crime, the message they send must be grossly offensive. Although many doxing cases contain grossly offensive messages (eg, making an image with photographs of a woman and her son on the entrance gate to the Auschwitz concentration camp), some of them may only include the target's contact information. As a result, cases of doxing that do not involve grossly offensive messages are not punishable under the MCA 1988.

The UK section 2A of the PHA 1997

Instead of giving a definition, section 2A (3) provides a list of acts that are associated with stalking, including following a person, contacting, or attempting to contact, a person by any means publishing any statement or other material relating to or purporting to relate to person, or purporting to originate from a person.[60] Additionally, the list is not exhaustive, so that courts may still consider various behaviors to be stalking even if they are not on the section 2A (3) list.[61]

According to PHA 1997 section 4A, in order to commit stalking crime, there should be at least two occasions. This means that there must be a course of conduct that amounts to harassment, and that particular harassment can be described as stalking behaviour.[62] However, doxing may occur on just one occasion.

Although the acts outlined in Article 2A(3) have a strong connection to doxing, defining conduct as doxing can face significant limitations due to the course of conduct requirement. In addition, doxing allows the cyberbullies to harass or harm the victim without actually stalking or following them. Consequently, existing UK legislation may help to prosecute some doxing cases, but it does not provide an appropriate and successful legal remedy for many forms of doxing.

Section 202(a) of the German Criminal Code (StGB): data espionage

Data espionage, also known as hacking, constitutes a criminal offense according to section 202(a) of the German Criminal Code (StGB).[63] Section 202(a) penalizes unlawfully obtaining data that are especially protected against unauthorized access with imprisonment not exceeding three years or fine. In order to commit the crime, the offender must access information system without permission and then obtain the data for himself/herself, or another person. No specified harm to occur required. Nonetheless, cyberbullies generally do not need access to information systems in order to dox their victims. Therefore, doxing cases that do not involve a hacking attack will not be punishable under section 202(a).

Section 202d of the StGB: handling stolen data

According to section 202(1), in order to commit the crime, offenders must either obtain data for themselves or another person, supply it to that person, distribute it, or in some other way grant access to it.[64] It states that acts must take place unlawfully for the purpose of harming others. However, no specified harm is required to occur. Considering these elements, it can be stated that, in doxing, cyberbullies also carry out acts that are prohibited in section 202(1) and therefore can be used against doxing. However, it should be noted that the data should be generally accessible. Such an approach may present challenges in combating doxing because cyberbullies frequently use data that have been released by victims.

Additionally, since 2007, persistent following or pestering of somebody, so-called stalking, has been a criminal offense according to section 238 of the German penal code.[65] Following the revision of section 238 in 2017, it was considered illegal to substantially harm the targeted person's lifestyle without supplying any proof of such harm.[66] The actual act that the offender takes towards the victim and the persistence of the act is the two factual elements of the stalking.[67] Different forms of acts and behavior that can be subsumed under stalking, such

59 *DPP v Paul Bussetti* [2021] EWHC 2140, CO/5022/2019 <https://www.bailii.org/ew/cases/EWHC/Ch/2021/2140.html> accessed 28 January 2023.

60 Section 2A of the Protection from Harassment Act 1997 <https://www.legislation.gov.uk/ukpga/1997/40/section/2A> accessed 28 January 2023.

61 For instance, even though there is no legal definition of cyberstalking to address the behaviour, the CPS stated that unwanted indirect contact with a person that may be threatening or menacing such as posting photographs of that person's children or workplace on a social media platforms, without any reference to the person's name or account constitutes cyberstalking and such a behaviour should be punished under the PHAs. 2A.The CPS, Stalking and Harassment <https://www.cps.gov.uk/legal-guidance/stalking-and-harassment> (13 May 2018) accessed 23 January 2023.

62 Section 4A of the Protection from Harassment Act 1997 <https://www.legislation.gov.uk/ukpga/1997/40/section/4A> accessed 28 January 2023.

63 Section 202(a), German Criminal Code (Strafgesetzbuch – StGB) <https://www.gesetze-im-internet.de/englisch_stgb/> accessed 23 January 2023.

64 Ibid s 202d.

65 Ibid s 238.

66 Anni Ropers and others, 'German Anti-Stalkin Legislation and its Recent Changes' (2020) 21 German Law Journal 788, 787–798.

67 Ibid 791.

as stalking another person in a manner suited to not insignificantly restricting that person's lifestyle, trying to establish contact with the other person by means of telecommunications or other means of communication or through third parties, improperly using the other person's personal data for the purpose of inducing third parties to make contact with that person, and threatening the other person, one of his or her relatives, or someone close to him or her with causing injury to life, or physical integrity, health, or liberty are prohibited in section 238(1–5). The offense further requires a conditional intent to commit the crime. This involves the perpetrator's intention to significantly affect the victim's lifestyle.[68] Additionally, section 238(8) states that the acts specified in paragraph 8 are not exhaustive and can be extended upon through interpretation. According to the German legislature's official justification for the law, persistence is expected to require continuous or repeated activity, which is not always demonstrated by simple repetition.[69] However, in most cases, section 238 may not apply to doxing, since section 238 requires a 'course of conduct' in order to commit the crime like other stalking acts.

Hong Kong Personal Data (Privacy) (Amendment) Ordinance 2021

Hong Kong has enacted an amendment that specifically addresses doxing. The Personal Data (Privacy) (Amendment) Ordinance 2021 (the Ordinance), was published in the Hong Kong Official Gazette on October 8th with the goal of criminalizing doxing and empowering the Privacy Commissioner to take action against it.[70] Article 64 3(A) of the Ordinance defines the offense of 'publication of personal data obtained without the agreement of data users' as the following:

> A person commits an offence if the person discloses any personal data of a data subject without the relevant consent of the data subject (a)with an intent to cause any specified harm to the data subject or any family member of the data subject; or (b)being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.

To effectively combat doxing, section 64 3(A) does not require a course of conduct in order to constitute a crime. Section 3(a) stipulates that the offense must be committed with intent to cause specified harm. Additionally, it provides exemptions if the disclosure is for lawful new activity or in the public interest. For instance, there is a difference between collecting and sharing the personal information of the victim who was stuck under the rubble after the earthquake and collecting the personal information of people belonging to an ethnic group that is under pressure in a country during wartime and posting it online. However, in both scenarios, the offenders could argue that their intention was to assist the victims, not harm them. On the other hand, simple expressions or materials including personal information that criticize politicians, rather than aim to harm them may also be penalized under this section, which could be used to suppress dissent. Therefore, in order to ensure a reasonable balance between protection of privacy and freedom of speech, it should be illuminated how the intention to harm will be proven.

It also requires two elements: first, the disclosure should be made without the data subject's relevant consent, and secondly, the disclosure should cause a specified harm. According to section 64(6/a), the term 'specified harm' encompasses a list of negative impacts or consequences that are considered harmful, including harassment, threat, intimidation, bodily harm, psychological harm, and causing the victim to be concerned about their safety. Regarding relevant consent, section 6 specifies who must give consent, however, it does not specify how consent should be obtained.[71] The general principles of the Ordinance may be expected to be applied in this case. The Ordinance prohibits the use of personal data for any new purpose that is not related to or unrelated to the original purpose when collecting the data, unless with the data subject's express and voluntary consent. In addition, data subject can withdraw their consent previously given by written notice. Furthermore, the data user should explain their purpose of obtaining the personal data to the data subject. It is not reasonable to assume that an individual gives consent to someone disclosing information about themselves so that it can be used against them for malicious purposes. Therefore, I

68 Andreas Mosbacher, Nachstellung s 238 StGB, Neue Zeitschrift für Strafrecht 669 (2007).

69 Bundestag-Drucksache 16/575, p 7.

70 The Personal Data (Privacy) Amendment Ordinance 2021 (8 October 2021) <https://www.pcpd.org.hk/english/data_privacy_law/amendments_2021/amendment_2021.html#:~:text=The%20Amendment%20Bill%20aims%20to,of%20disclosure%20of%20doxxing%20contents> accessed 25 January 2023.

71 According to s 64(3D) of the Ordinance, any person who is charged with a doxing offence contrary to the new s 64 of the Ordinance may adduce evidence to establish a defense pursuant to s 64(4) of the Ordinance If the person reasonably believed that the relevant consent of the data subject was obtained. However, it can be challenging to punish doxing when the defendant uses personal data that are made public by data subject.

do not believe that obtaining explicit non-consent to disclose personal information will be necessary in practice. Nevertheless, it can be stated that the Ordinance directly addresses doxing and seems to be an effective instrument against it.

Does data privacy law prohibit doxing? Limits on public data usage

However, doxing is directly related to data privacy law as it involves collecting or capturing someone's personal data and sharing or publishing it online. Data privacy law principles must be followed during the processing of personal data. These principles include that the data must be processed only for specific purposes and not used for any other purposes without the individual's consent. People often claim that doxing is not illegal since the data used for doxing such as names, photos, or phone numbers is already made public by individuals on the Internet.[72] However, the purpose limitation principle, which is a key aspect of data privacy law, dictates the opposite. This principle stipulates that personal data can only be collected and used for specific purposes, and any malicious dissemination of such information is a violation of privacy law.

In Turkish data privacy law, the general principles of data processing are stipulated in the Turkish Personal Data Protection Code (Data Code).[73] According to Article 5 of the Data Code, personal data shall not be processed without the explicit consent of the data subject. However, Article 5(2) (d) provides an exemption and states that if the data are made public by the data subject, they can be processed without the data subject's consent.[74] At first glance, it can be argued that most doxing cases cannot be punished under the Data Code since cyberbullies usually use data that have been made public by the data subject. In fact, personal data may only be processed in compliance with the procedures and principles of the Data Code and other laws. In other words, any processing of personal data that violate the general principles of the Data Code would be considered illegal. It is not reasonable to assume that an individual publishes information about themselves so that it can be used against them for malicious purposes. Even if the data subject publishes personal data with explicit consent, some of the rights attached to that data should still be protected. To illustrate this point, people can publish their information, such as their home address, phone number, or e-mail address on their LinkedIn account in order to allow potential employers to get an idea of who they are and connect with them. The fact that the data have been made public by the data subject should not give people the right to collect, give, or publish the data for malicious purposes. The information cannot be used for any purpose other than business. According to the Turkish Personal Data Protection Authority, the fact that data can be seen by others does not always imply that the data are completely public.[75] However, the term 'making public' has a narrower meaning within the scope of the Data Code and is directly related to the purpose for which the data subject made the information public.[76] For instance, the contact information published by a person who sells her vehicle on a website can only be used for the purpose of purchasing the vehicle or getting information about this advertisement; hence, using it for any other purposes (such as doxing) should be considered illegal. From this point of view, Article 136 of the Penal Code could be an effective tool to punish doxing cases.

In EU data privacy law, the definition of 'data made public by the data subject' is stated in Article 9(2) (e) of the GDPR.[77] Article 9(2) (e) provides an exceptional ground upon which 'sensitive' personal data may be processed without explicit consent if it relates to personal data that are manifestly made public by the data subject. However, it is important to note that even if the

72 Katherine Cross, '"Things have happened in the past week": on doxing, swatting, and 8Chan, Feministing' <http://feministing.com/2015/01/16/things-havehappened-in-thepast-week-on-doxing-swatting-and-8chan/> accessed January 26 2023.

73 7 April 2016 dated 6698 numbered Personal Data Protection Code. The objective of this Code is to protect fundamental rights and freedoms of persons, particularly the right to privacy, with respect to processing of personal data and to set forth obligations, principles, and procedures which shall be binding upon natural or legal persons who process personal data.

74 The 'Public Data' exception is stated in art 28/ç of the Turkish Data Code, and it states that data which are made public by data subject shall be processed without explicit consent.

75 Personal Data Protection Authority, 'Ruling about processing of personal data made public by the data subject for purposes other than making it public' <https://www.kvkk.gov.tr/Icerik/6623/2019-331> accessed 28 May 2022. The decision states that, even if the personal data of the Complainant are accessed through the website that was made public before, Since the Complainant's personal data are not used by the Company for the complainant's purpose of making it public, in other words, no attempt is made to reach the Complainant in order to benefit from his professional competence, on the contrary, it is understood that the Complainant is called with an appointment request regarding the Company's activities. It has been concluded that the data processing activity carried out by the Company cannot be evaluated within the framework of subparagraph (d) of paragraph (2) of art 5 of the Protection of Personal Data Code No 6698.

76 Personal Data Protection Authority, 'Notice about making data public', https://www.kvkk.gov.tr/Icerik/6843/-ALENILESTIRME-HAKKINDA-KAMUOYU-DUYURUSU

77 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

data are publicly available, the principles stated in Article 6 of the GDPR still apply, and a lawful basis needs to be established before using such data that are publicly available. The Article 29 Data Protection Working Party noted that personal data refer to any information relating to an identified or identifiable natural person, whether or not the information is accessible to the public.[78] Additionally, the Working Party states that such data have been made publicly available does not exempt it from the data protection law and its general principles.[79] Therefore, although publicly available information might be further processed under the GDPR without obtaining explicit consent, other obligations still exist and must be met. When an individual posts something on social media, it is generally assumed that they want it to be viewed by a wide audience. However, that does not mean that everyone can collect and use the data for malicious purpose. The collection and use of personal information from social media posts should be directly related to the reason why the information was made publicly available for which no consent is required to process. As a result, even if the data are made public by the data subject, they cannot be used to dox the data subject under the purpose limitation of the GDPR. Additionally, the Council of Europe Convention 108 also has a similar approach and prohibits the processing of data for illegal and incompatible purposes.[80]

UK data privacy law similarly recognizes the purpose limitation principle stated in Article 5(1)(b) of the GDPR. According to the Information Commissioner's Office, the fact that someone posted information on social media without limiting access does not entitle anyone to use it for other purposes.[81] In other words, the fact that data are publicly accessible does not imply that anyone has the right to use it for any reason, nor does it imply that the individual who posted the data has given their implicit consent to further use. What qualifies as 'manifestly made public' is not explicitly defined in the Data Protection Act 2018. However, it can be stated that the data subject should intentionally make the data public. Additionally, disclosures to a limited group of people are not always considered to be 'manifestly public'. In particular, being able to access information does not necessarily mean that it can be used for any purpose. Accordingly, for example, it is not considered public data if someone's credit card number appears in the background of a photo shared on social media or if someone posts their e-mail address with their connection on a professional network site. Consequently, the use of data made public by the data subject in order to dox people is prohibited under UK data privacy law as well.

In US law, there is no single data protection legislation. At the federal level, the Trade Commission Act (TCA) broadly empowers the US Federal Trade Commission (FTC) to bring enforcement actions to protect consumers against unfair or deceptive practices and to reinforce federal privacy and data protection regulations.[82] The FTC recommends privacy-by-design practices that include purpose specification and use limitation. Purpose specification means limiting data collection to that which is consistent with the context of a particular transaction or a consumer's relationship with the business, or as required or specifically authorized by law.[83] In other words, under the purpose specification principle, companies should specifically articulate the purpose or purposes for which personal information is intended to be used. On the other hand, use limitation refers to personal information that should be used solely for the purpose specified in the notice. The sharing of personal information should be for a purpose compatible with the purpose for which it was collected.[84] On this basis, it is possible to assert that some states adopt the purpose limitation in data processing. As a result, according to the TCA, even if the data used are made public by the data subject, disclosing personal information with malicious intent will violate these general principles. Nevertheless, the California Consumer Privacy Act, for example, provides no purpose or data minimization limits.[85] Thus, some states may need to adopt the purpose limitation in their legislation to prevent the use of public data for doxing.

Consequently, it can be stated that data privacy law prohibits disclosing personal data for malicious purposes, and regardless of whether the data are made public or not, it cannot be used to dox people under the purpose limitation principle.

78 Art 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (2 April 2013), 35.

79 Ibid 35.

80 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.

81 Information Commissioner's Office, 'Big data, artificial intelligence, machine learning and data protection' <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> accessed 30 January 2023.

82 Federal Trade Commission Act, <https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act> accessed 30 January 2023.

83 Center for Democracy and Technology, Refocusing the FTC's Role in Privacy Protection Comments of the Center for Democracy & Technology In regard to the FTC Consumer Privacy. Roundtable (6 November 2009), 4 <https://cdt.org/insights/refocusing-the-ftc%E2%80%99s-role-in-privacy-protection/> accessed 26 January 2023.

84 Ibid.

85 The California Consumer Privacy Act <https://theccpa.org/> 2018.

What legal values does doxing violate and why it is important for the future legislation?

People may voluntarily post private information about themselves online, but accessing all of the information that is stored in big data requires a thorough Internet search.[86] Cyberbullies with malicious intent use doxing as a tool by making personal information, which is hidden in this giant cyber cloud, more easily identifiable and accessible.[87] Previously stated, cyberbullies often use personal data as a weapon to cause harm, both physically and psychologically, to their targets, rather than just violating their privacy.

It can thus be seen that doxing involves more than just the right to privacy. Doxing has the potential to violate not only the right to privacy, but also the right to life, the right to physical integrity, the right to health, the right to safety, as well as human dignity. Therefore, in regard to doxing, the legally protected value should encompass more than just privacy. The Turkish Constitution recognizes 'the right to protect and develop material and spiritual entities', and it could be considered the legally protected value by penalizing doxing.[88] Accordingly, every individual has the right to protect and develop his or her spiritual existence by continuing his or her life and activities in a peaceful environment, without being disturbed, in a certain tranquility, psychological comfort, and serenity. It cannot be expected that people who are subject to doxing will be able to develop their material and immaterial selves.[89] In fact, the doxing subjects face harm every day, and thus they cannot be able to get a fresh start. Doxing is a threat that affects more than just data privacy. Thus, future legislation should consider that fact all of the above rights need to be protected. For this reason, it is necessary to focus on the existence of malicious intent and harm rather than focusing on elements such as whether the data are public or whether the consent of the data subject is obtained in doxing cases.

Conclusion

The advancement of technology has made publishing personal information online with malicious purpose a growing threat to individuals. Cyberbullies use doxing as a tool to harm (psychologically or physically), humiliate, or even kill their targets. While various cybercrime laws have been enacted in response to the growing threat of cyber threats, the issue of doxing has not received adequate attention.

Doxing involves collecting and disclosing personal data, which is considered data processing under data privacy law. Principally, personal data can only be processed with explicit consent from the data subject and under exceptional conditions. However, cyberbullies often claim that they use data that have already been published by the data subject, so that they don't need to obtain consent of the data subject. Despite claims to the contrary, this article revealed that the purpose limitation principle prohibits the use of personal information for doxing, regardless of whether the information is publicly accessible or not.

This article showed that the existing criminal approaches in the EU and US regions are inadequate for combating doxing because its applicability is limited, and terms are underinclusive and therefore, they may not cover all aspects of this harmful behaviour. Given the significant risks that doxing poses to individual privacy and security, it is crucial to establish effective legal measures. Hong Kong has taken an important step in this regard by directly prohibiting and enacting doxing into its legal system. In the EU, people can sue to have sensitive information pertaining to them removed from the Internet under the GDPR. This strategy could be applied to doxing. However, 'right to be forgotten' applies only when information is inaccurate, inadequate, irrelevant, or excessive, and it must be balanced against other fundamental rights such as the right to free speech.[90] For this reason, the form of the right to be forgotten may not address doxing. On the other hand, Germany

86 Big Data are massive amount of data that are growing exponentially over time. It is a data set that is so large and complex that no traditional data management tools can efficiently store or process it. *See* Youssra Riahi and Sara Riahi, 'Big Data and Big Data Analytics: Concepts, Types and Technologies' (2018) 5 International Journal of Research and Engineering 524.

87 Matthew James Enzweiler, 'Swatting Political Discourse: A Domestic Terrorism Threat' (2015) 90 Notre Dame Law Review 2001, 2007.

88 According to the Turkish Constitution art 17, everyone has the right to live, protect, and develop her/his material and spiritual entity. All freedoms are the results of the person's right to protect and develop his/her material and spiritual existence; it is interpreted as a hierarchy within the constitutional fundamental rights. Thus, the right to protect and develop the material and spiritual existence of the person, which is at the highest level of human rights, constitutes the reason for the existence of all freedoms as well as the purpose of human existence.

89 The Constitution was adopted by the Constituent Assembly on 18 October 1982, to be submitted to referendum and published in the Official Gazette dated 20 October 1982, and numbered 17844; republished in the repeating Official Gazette dated 9 November 1982 and numbered 17863 in the aftermath of its submission to referendum on 7 November 1982 (Act No 2709). *See* <https://www.anayasa.gov.tr/en/legislation/turkish-constiution/> accessed 5 April 2022.

90 David Erdos, 'The 'Right to be Forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps' (2021) 13 Journal of Media Law 1, at 11.

passed the Network Enforcement Act (NetzDG) in 2017. In the most general sense, NetzDG obligates the covered social media networks that have 2 million or more registered users in Germany to remove content that is 'clearly illegal' within 24 h after receiving a user complaint.[91] Even though doxing is not directly prohibited under German law, NetzDG could be effective to prevent doxing cases including hate speech or fake news which are clearly unlawful. However, doxing does not always include hate speech or fake news, which are the types of content that NetzDG covers.

However, the purpose limitation principle, which is a core element of data privacy law, prohibits the collection and disclosure of data for malicious purposes. As such, while the data privacy law provides the necessary legal framework to combat doxing, countries have not placed enough emphasis on combating doxing. Additionally, since doxing is a multifaceted threat that puts people's lives at risk, not just their privacy, there is a need for a comprehensive approach that directly prohibits and penalizes doxing, rather than solely relying on data privacy law. Therefore, future legislation should consider that doxing may violate many other fundamental rights apart from the right to privacy. Preventing doxing is essential for individuals to protect and develop their material and spiritual well-being.

Considering the challenges of the approaches reviewed, which may require a course of conduct to establish the crime, new legislation should broaden the definition of doxing to include a single act or a pattern of behaviour. This would allow for a more comprehensive approach to combat doxing, as individuals who engage in this harmful behaviour may not always exhibit a course of conduct that can be easily identified or proven in court.

Malicious intent is a key factor that distinguishes doxing from lawful expression, and new legislation should specify clear criteria for proving it in court.[92] The use of tools to search or investigate an individual's sensitive information can be helpful in proving malicious intent and holding doxers accountable for their actions. By including such provisions, legislation can strike a balance between the fundamental rights of privacy and freedom of expression, without causing disproportionate interference to either.

On the other hand, social media platforms have a significant role in preventing doxing, given that many incidents occur on these platforms. Social media platforms should develop and implement robust safeguards to protect their users against doxing. These safeguards should include both technological measures and policy guidelines to ensure that users' personal information is adequately protected. Technological measures such as AI-powered detection systems and moderation tools can be utilized to identify and remove doxing content promptly.

https://doi.org/10.1093/idpl/ipad011
Advance Access Publication 30 June 2023

91 S 1 of the Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG). 92 Douglas (n 18) 4.