

## Legal Protection for Victims of Cyberstalking According to Indonesia's Law



Leli Andespitrikasih<sup>1</sup>, Bambang Waluyo<sup>2</sup>, Beniharmoni Harefa<sup>3</sup>

<sup>1,2,3</sup>Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta

**ABSTRACT:** Using normative juridical methods, and legal, comparative and conceptual approaches, this research examines the protection of victims of cyberstalking crimes in Indonesia based on positive law. The progress of internet use in Indonesia from all sectors, whether using the internet for schools, business, or other communications, has made people freer to use internet access. However, this freedom will have a negative impact if there are no restrictions in the form of clear legal rules. The existence of the stalker phenomenon, where someone can obtain data anonymously and then carry out stalking, threats and other unpleasant acts that threaten life, are actions that can harm other people and are even dangerous actions. In Indonesia, cyberstalking is still included in the realm of ethics because there are no regulations that regulate it, so the author here is trying to formulate regulations that can become a legal basis for protecting victims of cyberstalking crimes according to several existing laws and regulations in Indonesia.

**KEYWORDS:** cyberstalking, victims, protection.

### INTRODUCTION

The rapid development of the times is characterized by changes in telecommunications and computer technology which are believed to have a positive impact on people's lives. This development can create a multifunctional Internet. This flexibility shows that the existence of internet technology can facilitate public information exchange.<sup>1</sup> Internet usage has increased rapidly. Apart from positioning information technology as a new media, it also facilitates communication and interaction between people.<sup>2</sup>

The positive impact of using social networks is that information can be accessed and shared more easily, the wider the network that is created, the easier it is to form communities that have a positive impact on society, increased crowdfunding and crowdsourcing activities, and many other positive effects. Apart from the positive impact, irresponsible use of the internet (especially social networks) can also have negative impacts. Various crimes can occur in cyberspace, which is now known as cybercrime.

Cybercrime is a crime that uses computer technology as the main means of crime. Cybercrime is a type of crime that takes advantage of developments in computer technology, especially the Internet.<sup>3</sup> One example of cybercrime is cyberstalking. Cyberstalking can be translated as stalking through cyberspace. Cyberstalking includes the act of using the internet, cellular telephone, and/or other means of communication to stalk another person. Cyberstalking can include false accusations, threats, impersonation, destruction of data or devices, solicitation of minors for sexual purposes, and any form of repeated insults. The act of cyberstalking includes covert movements in which a person obtains personal information about another person via the Internet, usually a social networking site.<sup>4</sup>

Cyberstalking can become a crime if it is not handled intensively.<sup>5</sup> Cyberstalking uses strategies and techniques to intimidate, humiliate, threaten, and control its targets. The reality is, cyber attackers know this technology well and there are many ways to abuse, harass, and threaten their targets. Cyberstalking can have many physical and emotional consequences for its victims

<sup>1</sup> Yiwei Gong, Jun Yang, Xiaojie Shi, "Towards a Comprehensive Understanding of Digital Transformation in Government: Analysis of Flexibility and Enterprise Architecture", *Government Information Quarterly*, Volume 37, Issue 3, July 2020, <https://doi.org/10.1016/j.giq.2020.101487>

<sup>2</sup> Mohammed T. Nuseir, Ghaleb Elrefae, "The Effects Of Facilitating Conditions, Costumer Experience And Brand Loyalty On Costumer-Based Brand Equity Through Social Media Marketing", *International Journal of Data and Network Science*, Volume 6, Issue 3, 2022, pp. 875-887. <https://doi.org/10.5267/j.ijdns.2022.2.009>

<sup>3</sup> Roy Eka Perkasa, Nyoman Serikat P, Bambang Eko Turisno, Perlindungan Hukum Pidana terhadap Konsumen dalam Transaksi Jual/ Beli Online (E-Commerce) di Indonesia, *Diponegoro Law Journal*, Volume 5, Nomor 4, 2016, hal. 1-3. <https://doi.org/10.14710/dlj.2016.13361>

<sup>4</sup> Rahel Octora, Problematika Pengaturan *Cyberstalking* (Penguntitan di Dunia Maya) dengan Menggunakan Annonymous Account pada Sosial Media, *Dialogia Iuridica*, Volume 11, Nomor 1, 2019, hal. 77-96. <https://doi.org/10.28932/di.v11i1.1902>

<sup>5</sup> Gurpreet Dhillon & Kane J. Smith, "Defining Objectives for Preventing Cyberstalking", *Journal of Business Ethics*, Volume 157, pp. 137-158, 2019. <https://doi.org/10.1007/s10551-017-3697-x>

## Legal Protection for Victims of Cyberstalking According to Indonesia's Law

online.<sup>6</sup> It is not uncommon for victims who are targeted to experience anger, fear and depression which can lead to death.<sup>7</sup> Cyberstalking carries out its actions via the internet by obtaining victims' personal data through social networks, such as names, addresses, family history, telephone numbers, information about daily routines, date of birth and other information. After obtaining personal data, the perpetrator repeatedly harassed the victim, such as making harassing telephone calls or leaving threatening messages to the victim through internet services. Apart from making threats, the perpetrator can misuse the victim's personal information or data by posting on websites or dating services related to sex while posing as the victim.<sup>8</sup>

A stalker will continue to try to find information about the victim's identity via the internet, personal archives, or other media that contain victim information, some even approach people close to the victim to obtain this without permission. In some cases, cyberstalking often even leads to doxing, which is a term that describes a situation where personal data that identifies a person is disseminated for certain purposes.<sup>9</sup> The data is in the form of the full name according to the Resident's Identity Card, gender, religion, marital status and other data which is then collected so that finally conclusions can be drawn and reveal who a person is in real life. If this data is collected, then that data will become a weapon to attack the victim.<sup>10</sup>

Before the Personal Data Protection Law was enacted, cyberstalking was purely an ethical matter. However, with the promulgation of the Law on Personal Data Protection (hereinafter abbreviated to the PDP Law), this act has become a criminal act which according to article 65 of the PDP Law is referred to as "collecting and disclosing personal data belonging to other people" with a criminal threat in accordance with article 67 of the Law PDP is a maximum prison sentence of 5 years and/or a maximum fine of IDR 5 billion. Cyberstalking can be categorized as a criminal act when there is forced interaction by the stalker on the victim, which causes feelings of fear and insecurity in the victim. Cyberstalking should be a criminal offense because it causes harm to other people and is carried out consciously and can be the first step to other criminal acts.

With the development of social media that are currently familiar such as Facebook, Twitter, Instagram, TikTok and others, it is also possible for this crime to occur through these media. Examples of the occurrence of cyberstalking in Indonesia include:<sup>11</sup> The case of Afriliyani, an ordinary citizen, suddenly became a hot topic of conversation when he was caught hitting 9 pedestrians. This is of course a violation that should be watched out for. However, what attracts attention is the reaction of Indonesian netizens or social media users who are known to be quick to respond to any issue. After Afriliyani's actions, everyone's comments were racist and tended to be insulting. Some comments even had a rather sensitive tone, as if they wanted to kill Afriliyani. Psychologically, Afriliyani and her family were devastated. There was even news that Afriliyani and her entire family were depressed and did not want to leave the house and stopped social activities like before. Apart from that, there is the case of a teacher from the Riau Islands who received harsh comments from his students on his Facebook account. The habits of a teacher who owns the social network Facebook and is known to students at the school have given rise to unfriendly comments on his Facebook. In fact, there are signs of threats and pressure. As a result of this action, the teachers experienced severe depression because every time they went to school, they always felt afraid. Another thing is what happened in the case of @KoprofiJati's Twitter which went viral because of his action of narrating a photo of the Indonesian first lady and the South Korean first lady at one of the G20 agenda sessions. In his tweet, the @KoprofiJati account mentioned the words employer and ART. This action received a response in the form of a 'digital attack', which is an act that cannot be justified. It cannot be denied that the Twitter account @KoprofiJati is indeed guilty. However, netizens who spread information in the form of combined data from Twitter accounts are clearly also guilty because this action is included in the Doxing act.

If you pay attention to the characteristics of cyberstalking, regulations should be regulated in such a way as to meet legal certainty. In this research, the problem will be discussed, namely how is the legal protection for victims of cyberstalking crimes according to positive law in Indonesia?

---

<sup>6</sup> Joanne D. Worsley, Jacqueline M. Wheatcroft, Emma Short, Rhiannon Corcoran, "Victim's Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses", *Sage Journals*, Volume 7, Issue 2, 2017, pp. 1-13. <https://doi.org/10.1177/2158244017710292>

<sup>7</sup> A. M. Chandrashekhar, Muktha G. S., & Anjana D. K., "Cyberstalking and Cyberbullying: Effects and Prevention Measures", *Imperial Journal of Interdisciplinary Research (IJIR)*, Volume 2, Issue 3, 2016, pp. 95-102. <http://www.onlinejournal.in>

<sup>8</sup> Irfa Khunainah, "Perlindungan Hukum terhadap Korban Cyberstalking di Media Sosial", terdapat pada <https://baladana.id/perlindungan-hukum-terhadap-korban-cyberstalking-di-media-sosial/>, diakses tanggal 16 Agustus 2023, Pukul 12.20 WIB.

<sup>9</sup> Batuhan Kukul, "Personal Data and Personal Safety: re-examining the limits of Public Data in the Context of Doxing", *International Data Privacy Law*, Volume 13, Issue 3, 2023, pp. 183-193. <https://doi.org/10.1093/idpl/ipad011>

<sup>10</sup> Deni Achmad, Muhammad Farid, Rasti Putri Januarti, Alyfia Syavira, "Legal Protection against Victims of Doxing Crime in Indonesia", *Jurnal Bina Mulia Hukum*, Volume 8, Nomor 1, 2023, hal. 92-105. <https://doi.org/10.23920/jbmh.v8i1.1062>

<sup>11</sup> Redaksi Justika, "Contoh Kasus Cyberstalking di Indonesia yang Perlu diperhatikan", terdapat pada <https://blog.justika.com/pidana-dan-laporan-polisi/contoh-kasus-cyberstalking-di-indonesia/>, diakses pada 10 Agustus 2023, pukul 11.30 WIB.

### RESEARCH METHODS

This research uses a normative juridical method because the focus in this research is the criminal law formulation policy regarding cyberstalking. Research on law using normative methods is carried out by identifying and conceptualizing law as norms, rules and regulations that apply to a certain sovereign country. Legal research using such an approach is normative legal research or doctrinal legal research.<sup>12</sup> This research uses approach methods, including legal approach,<sup>13</sup> comparative approach,<sup>14</sup> and conceptual approach. Based on its nature, this research is descriptive, namely research that is intended to provide data that is as accurate as possible about people, conditions, or other symptoms.

### DISCUSSION

The internet has penetrated every aspect of human life, including offices, schools, homes and entertainment centers.<sup>15</sup> From there, quite significant problems emerged, namely legal problems, faced by society regarding internet development.<sup>16</sup> Since the advent of the internet, two main forms have been distinguished, namely traditional stalking and cyberstalking.<sup>17</sup> Traditional stalking is a subcategory that is generally defined as a deliberate pattern of repeated, disruptive and intimidating behavior towards a specific person that causes the target to feel harassed, threatened and afraid. What characterizes stalking is the repeated or systematic nature of the behavior directed at a particular person. This behavior can be felt by the victim as disturbing, threatening, and causing fear.<sup>18</sup>

The definition of stalking itself can vary depending on the law or regulations that regulate it. However, in general, stalking is a form of criminal action that is carried out intentionally and individually, in various ways, including following someone repeatedly to harass that person, where the action is accompanied by threats of violence or death to create fear in oneself or to injure someone.<sup>19</sup> Cyberstalking is the use of the internet or other electronic means to harass a person, group of people, or organization by repeatedly sending harmful threats or intimidating messages.<sup>20</sup>

Linguistically, the word for protection in English is called protection. The term protection according to the KBBI can be equated with the term protection, which means the process or act of protecting, whereas according to Black's Law Dictionary, protection is the act of protecting.<sup>21</sup> In general, protection means protecting something from dangerous things, something that could be in the form of interests or objects or items. Apart from that, protection also contains the meaning of protection given by someone to someone who is weaker.<sup>22</sup> Thus, legal protection can be interpreted as all the government's efforts to ensure legal certainty to provide protection to its citizens so that their rights as citizens are not violated, and those who violate them will be subject to sanctions according to applicable regulations. The definition of protection is a place of refuge, things (actions and so on) that protect. In the KBBI, what is meant by protection is the method, process, and act of protecting. Meanwhile, law is a regulation made by the government or data that applies to everyone in society (the state).

Law enforcement efforts, including the government's efforts to provide legal protection. According to Philipus M. Hadjon, legal protection is the protection of dignity, recognition of the human rights of legal subjects according to statutory provisions, authority or as a set of rules and norms that can be protected.<sup>23</sup> He divided legal protection into 2 (two), namely preventative legal protection and repressive legal protection.

Legal protection for victims of cyberstalking crimes currently consists of several aspects, namely:

---

<sup>12</sup> Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990, hal. 4.

<sup>13</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, 2013, hal. 133-134.

<sup>14</sup> *Ibid.*, hal. 135.

<sup>15</sup> Alim Puspianto, "Realita Media Sosial dalam Kehidupan Cyber Society", *An-Nida': Jurnal Komunikasi dan Penyiaran Islam*, Volume 11, Nomor 2, 2023, hal. 49-73. <https://doi.org/10.61088/annida.v11i2.561>

<sup>16</sup> Andrea Sukmadilaga & Sinta Dewi Rosadi, "Upaya Hukum terhadap Pelanggaran Implementasi Internet of Things (IoT) di Bidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi", *Jurnal Suara Keadilan*, Volume 21, Nomor 2, 2020, hal. 205-221. <https://doi.org/10.24176/sk.v21i2.5694>

<sup>17</sup> Arvind Kumaar Gautam & Abhishek Bansal, "Impact Analysis of Feature Selection Techniques on Cyberstalking Detection". *Journal on Image Processing*, Volume 9, Issue 4, 2022, pp. 21-34. 10.26634/jip.9.4.19138

<sup>18</sup> Olga Cunha, Sonia Caridade, Telma C. Almeida, Rui Abrunhosa Goncalves, "Stalking Behaviors among Perpetrators of Intimate Partner Violence in Portugal: Correlates and Mediating Variables", *European Journal on Criminal Policy and Research*, Volume 29, 2023, pp. 147-165. <https://doi.org/10.1007/s10610-022-09511-z>

<sup>19</sup> Mira Marleni Pandie, Ivan Th. J. Weismann, "Pengaruh Cyberbullying di Media Sosial terhadap Perilaku Reaktif sebagai Pelaku maupun sebagai Korban Cyberbullying pada Siswa Kristen SMP Nasional Makassar", *Jurnal Jaffray*, Volume 14, Nomor 1, 2016, hal. 43-62. <http://dx.doi.org/10.25278/jj71.v14i1.188>

<sup>20</sup> Joseph Migga Kizza, "Cyberbullying, Cyberstalking, and Cyber Harassment", *Ethical and Secure Computing*, Springer, Chambridge, 2023, pp. 199-210. [https://doi.org/10.1007/978-3-031-31906-8\\_9](https://doi.org/10.1007/978-3-031-31906-8_9)

<sup>21</sup> Bryan A. Garner, *Black's Law Dictionary*, West, St. Paul 2009, hal. 1343.

<sup>22</sup> Ahmad Fauzi, Ismail Koto, "Tanggung Jawab Pelaku Usaha terhadap Konsumen terkait dengan Produk Cacat", *Journal of Education, Humaniora and Social Sciences (JEHSS)*, Volume 4, Nomor 3, 2022, hal. 1493-1500. <https://doi.org/10.34007/jehss.v4i3.899>

<sup>23</sup> Philipus M. Hadjon, *Loc.Cit.*

## Legal Protection for Victims of Cyberstalking According to Indonesia's Law

### 1. Aspects of Legal Substance (Preventive Efforts)

Preventative legal protection means allowing legal subjects to raise objections or opinions before the government makes a final decision. This is aimed at avoiding disputes.

### 2. Aspects of Legal Structure (Repressive Efforts)

Repressive legal protection is carried out after a problem occurs. Repressive legal protection attempts to resolve a problem so that the rights of every individual can be protected.

According to preventive and repressive legal protection, it can be seen as a manifestation of the objectives of law, namely upholding justice, certainty, order, benefit, and peace. Indonesia's constitution contains provisions to protect all citizens.

Amelia Putri and Eko Nurisman stated that the first step towards cybercrime in cyberspace is cyber stalking.<sup>24</sup> Cyberstalking involves stalking a target using advanced technology to gather information about the victim's personal information from all possible sources. Victims usually become targets of perpetrators because they hold personal grudges or are jealous.<sup>25</sup> To carry out their actions, cyber stalkers do not stalk the victim physically; conversely, cyberstalking uses social media networks to obtain the victim's personal information, which is then used against the victim.

Preventive and repressive legal protection can be seen as an embodiment of the objectives of law, namely upholding justice, certainty, order, benefit, and peace. Indonesia's constitution contains provisions to protect all citizens.<sup>26</sup> Every society has several rights that must be upheld. Every individual or group who is a victim of cybercrime, especially cyberstalking victims, has the same rights as those who are victims of physical crime. Apart from the provisions of the Legislative Regulations which have been described in the previous problem formulation - the Criminal Code, Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, and Law of the Republic of Indonesia Number 27 of 2022 on Protection of Personal Data.

There are quite a lot of laws that regulate the protection of victims when viewed from the perspective of Indonesian positive law. In this case, the highest constitution, the 1945 Constitution, regulates the rights of all people in general. Article 28 of the 1945 Constitution outlines the requirements for protecting individual rights. Everyone has inalienable rights because they are human beings. The protection of individual rights from various sources is regulated by positive law such as the Criminal Procedure Code (KUHAP), the Human Rights Law (HAM), and the ITE Law, in addition to the basic rights guaranteed by the Law, 1945 Constitution.

In addition, several laws are still not sufficient to accommodate or protect victims of cyberstalking crimes, even though there are many regulations governing victim protection. If we look closely, we will find that the only laws that expressly regulate technology-related behavior - in this case, cyberstalking - are the ITE Law and the Human Rights Law. Some laws only regulate how a person's rights are protected generally and when it comes to actions carried out without the use of technology. Article 13, Article 14, Article 23, and Article 32 of the Human Rights Act are the only places where the rules governing technology are relevant in this situation. Apart from that, as regulated in Law Number 13 of 2006 concerning Protection of Witnesses and Victims, perpetrators who endanger victims of technology crimes also have the right to receive legal protection in certain circumstances (UU PSK).

Furthermore, it is stated that "a victim is someone who experiences physical, mental suffering and/or economic loss as a result of a criminal act" in Article 1 paragraph (2) of the PSK Law. In this case, those who experience both material and non-material losses due to cybercrime can be said to be victims. Basically, there are two models for providing legal protection to cybercrime victims: the procedural rights model and the service model:<sup>27</sup>

#### 1) The Procedural Rights Model

The procedural rights model expressly provides victims of cybercrime with the ability to "get back" at those who have wronged them by giving them the ability to report crimes, cooperate with law enforcement, and attend all court proceedings where their testimony is required. Victims are also expected to participate more actively in assisting law enforcement officials with their cases under this procedural model, especially in the case of contemporary cybercrime. The existence of procedural rights can also restore the victim's trust after he or she has been harmed by irresponsible parties (the defendant), apart from that this can also be a consideration for the public prosecutor in the event that the prosecutor provides charges that are too light.

---

<sup>24</sup> Amelia Putri Anisah dan Eko Nurisman, *Loc.Cit.*

<sup>25</sup> Nurzakiah Simangunsong, Novita Sari, Hasna Dewi Ritonga, Mara Zona, "Peran Guru dalam Mengatasi Bullying di SD Negeri 200117/26 Padangsidempuan", *Journal of Educational Research and Practice*, Volume 1, Nomor 1, 2023, hal. 113-123. Retrieved from <https://cesmid.or.id/index.php/jerp/article/view/107>

<sup>26</sup> Rafina Rafina, Akhhmad Zaki Yamani, "Peran Konstitusi dalam Demokrasi dan Hak Asasi Manusia di Indonesia", *Causa: Jurnal Hukum dan Kewarganegaraan*, Volume 2, Nomor 11, 2024, hal. 1-12. <https://doi.org/10.3783/causa.v2i11.2551>

<sup>27</sup> Muladi dan Barda Nawawi Arif, *Bunga Rampai Hukum Pidana*, Alumni, Bandung, 1992, hal. 79.



## Legal Protection for Victims of Cyberstalking According to Indonesia's Law

### 2) The Service Model

Developing uniform standards for victims of cybercrime is a key focus of this service model. According to this model, cybercrime victims are people who need to be served by the police and other law enforcement officials. If law enforcement officers provide effective services to victims of cybercrime, it will have a positive impact on law enforcement in general and cybercrime in particular. As a result, victims of technological advances will trust law enforcement institutions more when they provide services to victims, because they feel that their rights are protected, and their interests are guaranteed. Because cybercrime is a modern crime that requires serious attention from the government because cybercrime will have an impact on the real world, law enforcement officials must prepare human resources who can be trusted and understand technology. This is very important, especially when it comes to proving cybercrimes in court. Many cases arise due to developments in information technology. The ITE Law and PDP Law are expected to help law enforcement in protecting individuals who use technology.

To ensure that every citizen is safe and protected in cyberspace, the country created the ITE Law, a special law. Everyone has limitations in their activities in cyberspace thanks to the ITE Law, an excellent breakthrough produced by the government. As an illustration, Article 28 of the ITE Law states that spreading hate speech and false information online is an act against the law. This allows anyone to do whatever they want because life in cyberspace is so free without knowing the boundaries of space and time. In addition, additional regulations are also included in the ITE Law to protect all parties, as stated in Articles 27 to 37. Even with the ITE Law, not all cybercrime victims are well protected. However, in practice, strong collaboration from various parties is needed to combat and protect victims of cybercrime.

Based on this, there are important steps that can be taken by Indonesia to tackle cyberstalking crimes, namely:

1. By modernizing and creating special rules and detailed implementing regulations related to cyberstalking crimes.
2. There is maintenance and improvement of the national computer network security system.
3. Increasing public awareness of cybercrime is very necessary. It should be noted that there are still many Indonesian people who are still unfamiliar with crime.

## CONCLUSION

In terms of legal protection, there are preventive and repressive efforts that can be carried out to protect the interests of victims. Apart from the regulations above as rules, prohibitions and sanctions for cyberstalking perpetrators, the state also has regulations which contain basic human rights, living in peace and prosperity based on the inherent rights of human rights which have been written in the 1945 Constitution and the Laws Human Rights Law, as well as obtaining protection from the authorities for the offense of Complaints and based on the Criminal Procedure Code. In addition, victims in this case are required to always be supervised and protected based on the Witness and Victim Protection Law. Basically there are two models of approaches that can be used to legally protect victims of cybercrime: 1) procedural rights model, where the victim has the right to participate in all stages of the legal process and can assist the prosecutor in carrying out the prosecution; 2) service model, which views victims as people who need to be served by the police and other law enforcement officers so that victims feel their interests are protected fairly. Assistance for victims of cybercrimes and physical crimes must be provided at every stage of the investigation, trial and post-trial processes.

## REFERENCES

- 1) M. Chandrashekhar, Muktha G. S., & Anjana D. K., "Cyberstalking and Cyberbullying: Effects and Prevention Measures", *Imperial Journal of Interdisciplinary Research (IJIR)*, Volume 2, Issue 3, 2016, pp. 95-102. <http://www.onlinejournal.in>
- 2) Ahmad Fauzi, Ismail Koto, "Tanggung Jawab Pelaku Usaha terhadap Konsumen terkait dengan Produk Cacat", *Journal of Education, Humaniora and Social Sciences (JEHSS)*, Volume 4, Nomor 3, 2022, hal. 1493-1500. <https://doi.org/10.34007/jehss.v4i3.899>
- 3) Alim Puspianto, "Realita Media Sosial dalam Kehidupan Cyber Society", *An-Nida':Jurnal Komunikasi dan Penyiaran Islam*, Volume 11, Nomor 2, 2023, hal. 49-73. <https://doi.org/10.61088/annida.v11i2.561>
- 4) Andrea Sukmadilaga & Sinta Dewi Rosadi, "Upaya Hukum terhadap Pelanggaran Implementasi Internet of Things (IoT) di Bidang Pelayanan Kesehatan Menurut Ketentuan Perlindungan Data Pribadi", *Jurnal Suara Keadilan*, Volume 21, Nomor 2, 2020, hal. 205-221. <https://doi.org/10.24176/sk.v21i2.5694>
- 5) Arvind Kumar Gautam & Abhishek Bansal, "Impact Analysis of Feature Selection Techniques on Cyberstalking Detection". *Journal on Image Processing*, Volume 9, Issue 4, 2022, pp. 21-34. 10.26634/jip.9.4.19138
- 6) Batuhan Kukul, "Personal Data and Personal Safety: re-examining the limits of Public Data in the Context of Doxing", *International Data Privacy Law*, Volume 13, Issue 3, 2023, pp. 183-193. <https://doi.org/10.1093/idpl/ipad011>
- 7) Bryan A. Garner, *Black's Law Dictionary*, West, St. Paul 2009.
- 8) Deni Achmad, Muhammad Farid, Rasti Putri Januarti, Alyfia Syavira, "Legal Protection against Victims of Doxing Crime in Indonesia", *Jurnal Bina Mulia Hukum*, Volume 8, Nomor 1, 2023, hal. 92-105. <https://doi.org/10.23920/jbmh.v8i1.1062>

## Legal Protection for Victims of Cyberstalking According to Indonesia's Law

- 9) Gurpreet Dhillon & Kane J. Smith, "Defining Objectives for Preventing Cyberstalking", *Journal of Business Ethics*, Volume 157, pp. 137-158, 2019. <https://doi.org/10.1007/s10551-017-3697-x>
- 10) Irfa Khunainah, "Perlindungan Hukum terhadap Korban Cyberstalking di Media Sosial", terdapat pada <https://baladena.id/perlindungan-hukum-terhadap-korban-cyberstalking-di-media-sosial/>, diakses tanggal 16 Agustus 2023, Pukul 12.20 WIB.
- 11) Joanne D. Worsley, Jacqueline M. Wheatcroft, Emma Short, Rhiannon Corcoran, "Victim's Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses", *Sage Journals*, Volume 7, Issue 2, 2017, pp. 1-13. <https://doi.org/10.1177/2158244017710292>
- 12) Joseph Migga Kizza, "Cyberbullying, Cyberstalking, and Cyber Harassment", *Ethical and Secure Computing*, Springer, Chambridge, 2023, pp. 199-210. [https://doi.org/10.1007/978-3-031-31906-8\\_9](https://doi.org/10.1007/978-3-031-31906-8_9)
- 13) Mira Marleni Pandie, Ivan Th. J. Weismann, "Pengaruh Cyberbullying di Media Sosial terhadap Perilaku Reaktif sebagai Pelaku maupun sebagai Korban Cyberbullying pada Siswa Kristen SMP Nasional Makassar", *Jurnal Jaffray*, Volume 14, Nomor 1, 2016, hal. 43-62. <http://dx.doi.org/10.25278/jj71.v14i1.188>
- 14) Mohammed T. Nuseir, Ghaleb Elrefae, "The Effects Of Facilitating Conditions, Costumer Experience And Brand Loyalty On Costumer-Based Brand Equity Through Social Media Marketing", *International Journal of Data and Network Science*, Volume 6, Issue 3, 2022, pp. 875-887. <https://doi.org/10.5267/j.ijdns.2022.2.009>
- 15) Muladi dan Barda Nawawi Arif, *Bunga Rampai Hukum Pidana*, Alumni, Bandung, 1992.
- 16) Nurzakiah Simangunsong, Novita Sari, Hasna Dewi Ritonga, Mara Zona, "Peran Guru dalam Mengatasi Bullying di SD Negeri 200117/26 Padangsidempuan", *Journal of Educational Research and Practice*, Volume 1, Nomor 1, 2023, hal. 113-123. Retrieved from <https://cesmid.or.id/index.php/jerp/article/view/107>
- 17) Olga Cunha, Sonia Caridade, Telma C. Almeida, Rui Abrunhosa Goncalves, "Stalking Behaviors among Perpetrators of Intimate Partner Violence in Portugal: Correlates and Mediating Variables", *European Journal on Criminal Policy and Research*, Volume 29, 2023, pp. 147-165. <https://doi.org/10.1007/s10610-022-09511-z>
- 18) Peter Mahmud Marzuki, *Penelitian Hukum*, Kencana Prenada Media Group, Jakarta, 2013.
- 19) Rafina Rafina, Akhhmad Zaki Yamani, "Peran Konstitusi dalam Demokrasi dan Hak Asasi Manusia di Indonesia", *Causa: Jurnal Hukum dan Kewarganegaraan*, Volume 2, Nomor 11, 2024, hal. 1-12. <https://doi.org/10.3783/causa.v2i11.2551>
- 20) Rahel Octora, *Problematika Pengaturan Cyberstalking (Penguntitan di Dunia Maya) dengan Menggunakan Annonymous Account pada Sosial Media*, *Dialogia Iuridica*, Volume 11, Nomor 1, 2019, hal. 77-96. <https://doi.org/10.28932/di.v11i1.1902>
- 21) Redaksi Justika, "Contoh Kasus Cyberstalking di Indonesia yang Perlu diperhatikan", terdapat pada <https://blog.justika.com/pidana-dan-laporan-polisi/contoh-kasus-cyberstalking-di-indonesia/>, diakses pada 10 Agustus 2023, pukul 11.30 WIB.
- 22) Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*, Ghalia Indonesia, Jakarta, 1990, hal. 4.
- 23) Roy Eka Perkasa, Nyoman Serikat P, Bambang Eko Turisno, *Perlindungan Hukum Pidana terhadap Konsumen dalam Transaksi Jual/ Beli Online (E-Commerce) di Indonesia*, *Diponegoro Law Journal*, Volume 5, Nomor 4, 2016, hal. 1-3. <https://doi.org/10.14710/dlj.2016.13361>
- 24) Yiwei Gong, Jun Yang, Xiaojie Shi, "Towards a Comprehensive Understanding of Digital Transformation in Government: Analysis of Flexibility and Enterprise Architecture", *Government Information Quarterly*, Volume 37, Issue 3, July 2020, <https://doi.org/10.1016/j.giq.2020.101487>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.