Universitas Warmadewa

Editorial Office: Department of Government | Faculty of Social and Political Sciences | Universitas Warmadewa

Jl. Terompong No.24, Sumerta Kelod, Kec. Denpasar Timur, Kota Denpasar, Bali 80239

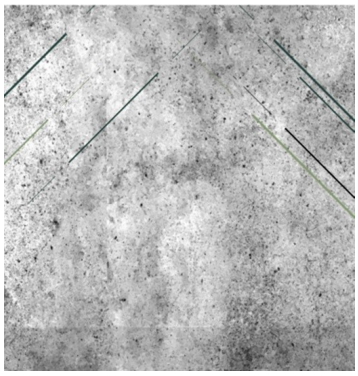
Politicos: Jurnal Politik Dan Pemerintahan

Volume 4, Number 1, 2024

ISSN: 2776-8031 (Print) | 2776-8023 (Electronics)

Publication details, Including author guidelines

Visit URL: https://www.ejournal.warmadewa.ac.id/index.php/politicos/onlinesubmissionandauthorguideline



Digital Security in Human Security: A Case Study of the Bjorka Hacking Incident

Nadia Varayandita Ingrida, Dody Wibowo

Universitas Gadjah Mada

Article History

Received : December 28, 2023

Revised : Januari 2, 2024

Accepted : March 10, 2024

How to cite this article (APA)

Ingrida, N. V., & Wibowo, D. (2024). Digital Security in Human Security: A Case Study of the Bjorka Hacking Incident. *Politicos: Jurnal Politik Dan Pemerintahan*, 4(1), 33-44. https://doi.org/10.22225/politicos.4.1.2024.56-65

ISSN 2776-8031 (Print)
ISSN 2776-8023 (Electronics)

POLITICOS

Original Article

Volume 4 Number 1 (2024)
https://doi.org/10.22225/politicos.4.1.2024.56-65

Digital Security in Human Security: A Case Study of the Bjorka Hacking Incident

Nadia Varayandita Ingrida, Dody Wibowo*
Universitas Gadjah Mada

Abstract

The issue of human security in the digital era has garnered attention in line with technological advancements. The threats to individual privacy and security have become increasingly evident, particularly following the hacking incident by Bjorka in September 2022 in Indonesia. This research applies the concept of human security within the context of digital security, highlighting the inequalities in access and vulnerabilities in online privacy. The Bjorka case reflects the complexity of human security, encompassing freedom from fear, freedom from want, and the freedom to live in dignity concerning the fundamental rights of individuals in human security. The aim of this study is to understand the privacy breaches and data hacking conducted by Bjorka and its impact on the human security of Indonesian citizens, especially from the perspective of digital security. This case study research employs interviews with key respondents from diverse backgrounds, who may have been victims of Bjorka's hacking. The study finds that digital security is not only related to technical aspects but also involves disrupted human security issues, pertaining to basic human rights, access limitations, and the gender identity of individuals involved in the digital world.

Keywords: Human Security; Digital Security; Hacking; Bjorka

Introduction

Human security embodies a condition where individuals are granted justice in terms of access to services and opportunities that enable them to live with dignity and prosperity. The concept of human security has evolved alongside the advent of digital technology. According to Rachman and Susan (2021), in the study of peace and conflict resolution, actions by digital actors can endanger both traditional security, which focuses on the state, and non-traditional security, which focuses on citizens/humans. This underscores the need for heightened attention to digital security in the face of technological advancements. Personal data, directly linked to individuals, is vulnerable to cyber threats, exacerbated by a lack of individual understanding about privacy and digital access challenges.

In September 2022, a significant digital data breach occurred in Indonesia by Bjorka, a member of the "Breached Forums." The breach began with the dissemination of sensitive data obtained after stealing information from Tokopedia and Wattpad in April and June 2020 (Shiba, 2022). Bjorka then stole more sensitive data in August–September 2022, including data on 26 million Indihome customers, 1.3 billion SIM card data, 3.2 billion Peduli Lindungi data, and 105 million KPU data, which were then sold on the Breached.to site (CNN Indonesia, 2022). Pratama Persadha, a researcher at the Cyber Security Research Center CISSReC, confirmed that the hacked data was valid (Saptohutomo, 2022).

Weaknesses in security systems can open the door to privacy violations that harm individuals and threaten human security in the digital world. Therefore, this research aims to understand the impact of privacy breaches and data hacking by Bjorka on the human security of Indonesian citi-

*Corresponding author: Dody Wibowo. Universitas Gadjah Mada
Bulaksumur, Caturtunggal, Kec. Depok, Kab. Sleman, Daerah Istimewa Yogyakarta, 55281 Indonesia
Email: dwibowo@ugm.ac.id

zens from a digital security perspective. Like any other human-inhabited space, the digital world is not immune to chaotic and frightening situations, thus human security can face threats from various directions (Candra & Wardoyo, 2020). Although digital security is generally considered to affect an unseen and intangible space, it has very real implications in the physical world (Klein & Hossain, 2020). Digital security has become a concern encompassing overall human security, and the digital access gap introduces a new understanding of the losses suffered by data breach victims, such as the risk of future injury and anxiety due to data breaches (Solove & Citron, 2017). Therefore, this issue is no longer just a technical problem but is closely related to human security and welfare. Digital security becomes a controversy that creates new challenges in managing human security, especially in the context of personal data privacy, as the vast amount of data is likened to "the new oil," meaning that the collected data is a potential asset that can be misused.

The case of data hacking by Bjorka has not been specifically discussed using the Human Security lens. The majority of the literature found discusses privacy in the context of law and informatics disciplines. Literature by Indah, Sidabutar, and Annisa (2022) portrays Bjorka's hacking as a threat of digital invasion and data exchange in the digital era. Kurnia (2023) highlights issues of hacktivism and personal data protection in Indonesia, marking the need for improvements in data protection in the future. Anantaka, Zulfa, and Nita (2023) in their research discuss community support for Bjorka's actions. Farhan and Cindy (2023) discuss inequalities in understanding cyber security and the effectiveness of the Personal Data Protection Act in Indonesia. Finally, Sukmawan and Setyawan (2023) discuss the role of the government and companies in maintaining data security and citizen privacy. Based on these literatures, the novelty of this research is the use of the Human Security lens on digital security concerning privacy in large-scale data management and its connection with the inequality of digital access.

The evolution of human security in digital security highlights the cross-border nature of traditional and non-traditional areas, introducing the concept of cyberspace as an integral part of a country's or region's physical territory (Soewardi, 2013). The rapid development of the internet opens up an understanding of a virtual world that crosses national boundaries, reflecting the complexity of the concept of territory in the digital era (Cahyadi, 2018). Meanwhile, this evolution brings about the era of Society 5.0, which opens new opportunities and risks, such as hacking that can threaten individual data privacy (Halimawan et al., 2020). Digital equality is key to ensuring that technology and information can be accessed fairly by all individuals, regardless of their background or level of digital access (Bachtiar et al., 2020).

The importance of data privacy and digital access is closely related to three aspects of human security: freedom from fear, freedom from want, and the freedom to live in dignity (Wardoyo, 2015). Human security in the digital era requires protection against data privacy breaches, with freedom from fear related to data breach threats and associated risks, freedom from want encompassing equal access to technology, and freedom to live in dignity connected to the individual's right to live without the interference of personal information misuse (Lauermann, 2022). Thus, digital security is not just about protecting systems and data, but also involves efforts to ensure equality, freedom, well-being, and dignity of individuals in an increasingly complex digital environment. Through the lens of human security, this research aims to enrich the wider discussion on human security in the digital age, underscoring the necessity for holistic strategies that safeguard individual rights amidst the evolving landscape of digital threats.

Method

This research is a case study focused on human security in the digital space, particularly in the context of the Bjorka hacking incidents. The selection of this method is based on its ability to provide insights into the subjective experiences and perceptions of respondents regarding digital security and the impact of hacking, especially in relation to the Bjorka case. Victims of Bjorka's hacking are spread across various regions. In this study, the chosen respondents for interviews, although not necessarily victims of the Bjorka hacking case, have experienced hacking incidents. The respondents, totaling twenty individuals comprising ten women and ten men, reside in the

the Special Region of Yogyakarta. This location was selected due to its high level of information and computer technology skills, with 84.72% of its population skilled in these areas, ranking it third in Indonesia in 2021 (Ridwan, 2022).

Data collection methods include interviews, digital observation, and documentation as primary data, with secondary data obtained from digital surveys, scientific articles, journals, news, social media, books, and related documents. The selection of interview respondents utilized purposive and snowball sampling techniques. Purposive sampling targets individuals directly affected by hacking or those with specific knowledge about the Bjorka hacking case, including those who have been hacking victims or are knowledgeable about the Bjorka case, as well as representatives from DISKOMINFO DIY, digital security practitioners, and Jogja Cyber Security representatives. Meanwhile, snowball sampling allows researchers to access key informants not identified at the study's outset by expanding the respondent network through recommendations from initial informants. This technique aids in identifying more hacking victims who have experienced similar impacts or possess relevant knowledge about digital security and the Bjorka hacking case.

Results

Bjorka remains a hot topic and subject of intense discussion among the Indonesian public due to the hacking incidents they have carried out. However, the reason behind choosing the name Bjorka remains unclear. Some speculations point to several countries, including Sweden, because names like Bjork, Bjorck, or Bjork are Swedish family names, Iceland for the word Birch (a girl's name), and it is also recorded as a family name in the United States, Canada, Minnesota, and Poland (Putsanra, 2022). According to information technology experts, Bjorka is part of a group of people in Indonesia from Tanjung Pura Cirebon and Madiun, as seen from their English writing style (Gustiana, 2022). However, on the Twitter account (X), Bjorka claims to be from Warsaw, Poland (Shiba, 2022). With a mysterious and confusing identity, Bjorka has managed to keep secrets about themselves amidst public attention to their hacking cases. Bjorka used the Twitter account (X) @bjorkanism to spread their actions, and although the account was relatively new, created on Friday, September 9, 2022, it successfully gained 135,000 followers. However, on Monday, September 12, 2022, the account was suspended for violating rules. The Bjorkanism Telegram channel has 48,000 members and is used by Bjorka to distribute the hacked data in full or as samples. This facilitates the rapid dissemination of information and integrity that is inherent to individuals (Brown & Esterhuysen, 2019).

Bjorka not only hacked data but also sold it on Breached.to, a domain connected to Breached Forums. There, a specific marketplace exists, the Leaks Market, where leaked data is sold for cryptocurrencies such as Ethereum or Bitcoin (Hardiansyah, 2022). This action reflects insecurity in the cyber realm (Candra & Wardoyo, 2020) that can impact the physical world, such as extortion and fraud through WhatsApp directing to download applications. As a result, individuals feel unsafe from threats that disturb their security. Thus, the Bjorka case can be considered a criminal act that threatens human security. Bjorka's activities have led to distrust in data security and created concerns about the potential for greater digital crimes. Debates and social tensions arise along with the motivations of Bjorka's hacking, viewed by some as a form of free speech, while others see it as digital criminality. The involvement of the general public in digital life also comes under scrutiny, with the potential risk of their data being misused indirectly. These impacts threaten freedom from fear and the right to live free from disruptive threats in the digital realm.

The threat to human security is interconnected in a domino effect (Tadjbakhsh, 2014). To have profound meaning, human security must be considered at a more personal level in people's daily lives (Tadjbakhsh, 2014), such as in the use of digitalization and the threat of hacking crimes. The presence of hacking crimes presents challenges in defining boundaries in cyberspace (Gani, 2023). Hacking falls under cybercrime because states have cyber sovereignty, an extension of territorial sovereignty established by infrastructure with consequences for a country's legal jurisdiction and administrative protection. The hacking cases carried out by Bjorka expose vulnerabilities in digital data security protection directly related to individuals and sensitive to criminal acts like

https://doi.org/10.22225/.politicos.4.1.2024.56-65

hacking that occur in physical territories or countries. Like places inhabited by humans, the digital world is not exempt from chaotic and frightening situations and conditions, threatening human security from various directions.

In this research, the authors explore the three freedoms that are core to human security: freedom from fear, freedom from want, and freedom to live in dignity as guidelines, and to create an environment safe from threats and underpinning the fundamental rights of individuals in the digital era. By detailing each freedom and the responses of the respondents, it can be understood how digital security is not only a technical issue but also relevant to the protection of fundamental human rights in the digital world.

Freedom from Fear

The concept of freedom from fear emphasizes the human security need to be free from the fear of crime (Alkire, 2003), and liberates individuals to live their lives fully as human beings (Hidayat, 2017). All twenty respondents expressed fear of hacking into their personal data, which could make them victims of criminal acts. A male respondent said that he is aware of the case and suspects he might have fallen victim to it, especially since his information was included in the application that was compromised. He suspects his data might have been sold for online loan purposes, given the numerous calls he's received from strangers. He has yet to file a report, primarily due to uncertainty about the reporting process. His statement about receiving several phone calls from unknown individuals reflects his concern over feeling threatened, not just physically, but also in terms of emotional and mental protection.

Another male respondent reported a scam in June 2023, where an impersonator accessed his and his classmate's data, possibly through hacking. Two numbers, falsely claiming to be him and another classmate, joined their high school group chat under the guise of new phone numbers. These impersonators quickly began soliciting mobile credit from classmates, with requests exceeding 100k, under the promise of repayment by noon. The scam led to confusion and a significant loss for one individual who sent 202k worth of credit, based on a profile picture from the respondent's Instagram. This incident raised concerns about data security, resulting in financial loss and feelings of intimidation among the victims.

A female respondent stated that she is aware of Bjorka but has not been, and hopes never to be, affected by the hacking. She shares the anxiety regarding Bjorka's hacking of personal data. She has never reported it because she still feels her data is safe. However, she remains cautious and vigilant, careful not to carelessly click on anything on the internet. This has raised concerns, as incidents of personal data breaches often reveal that no data storage system is completely immune to hacking threats (Arif & Chania, 2022), even for those who believe their data is secure. Once an individual has entered their data into a platform, they have, in effect, shared their data and it becomes susceptible to hacking. Various methods and actions can be undertaken to hack or manipulate data within a system without the owner's consent (Arif & Chania, 2022).

Freedom from Want

Although the impact is indirect, the concept of freedom from want must be emphasized as a significant effect of the Bjorka hacking, directly related to freedom from fear. Freedom from want refers to chronic threats like hunger, disease, and oppression, as well as protection from sudden and dangerous disruptions in daily life at home, work, or in society (UNDP, 1994). Sudden and dangerous disruptions, in the context of freedom from want, include unpredictable crimes like Bjorka's hacking, which can affect daily needs for food, health, and protection. Freedom from want in human security focuses on the right of every individual to live without deprivation, securing basic needs such as food, clean water, housing, education, healthcare, and other fundamental aspects of life (Siahaan, 2004). It underscores the importance of social justice as the foundation for maintaining overall human well-being (Siahaan, 2004).

This concept not only refers to freedom from hunger or material shortage but also to well-being that ensures individuals are free from fear and anxiety rooted in unmet basic needs. In the

current context of digital security, protection increasingly specializes against the occurrence of digital crimes (Ardiyanti, 2016). Protecting personal data and digital infrastructure becomes crucial given the high level of human dependence on technology.

Interviews with respondents revealed their concerns about digital security and the desire for freedom from want, a key aspect of human security that encompasses the right to live without deprivation and access basic needs. All respondents indicated that hacking affects their economic security, particularly because there's a risk that their hard-earned money, used to meet daily living needs, could be stolen, leaving them unable to maintain a decent standard of living. A male respondent recounted an incident where his personal data, potentially compromised by Bjorka, led to a fraudulent job offer requiring a deposit, an event he chose not to report due to its complexity. Another male respondent shared his experience of being impersonated and threatened after his photo was used to deceive his friends, highlighting the fear and anxiety such digital crimes provoke.

A female respondent mentioned hearing about Bjorka and experiencing suspicious calls and messages, suggesting a breach of her personal data. Her mother was tricked into applying for a credit card, leading to unwarranted bills and harassment from debt collectors, despite not using the card. These accounts underscore the importance of protecting personal data and digital infrastructure to prevent digital crimes that threaten individuals' well-being and financial security, aligning with the concept of freedom from want by ensuring safety from the fear and anxiety caused by unmet basic needs in the digital age.

Freedom to Live in Dignity

Freedom to Live in Dignity within the context of digital security emerges due to a domino effect on individuals related to threats and the hacking activities of Bjorka, impacting both freedom from fear and freedom from want. Threats range from clear and immediate dangers to chronic violations against human dignity (Tadjbakhsh, 2014). Living with dignity refers to the right of every individual to live with self-respect, honor, and a decent quality of life (Komnasham.go.id, n.d.). All respondents expressed that their dignity could be compromised due to the hacking of their personal data. The dissemination of private information, such as their personal photos, by hackers could lead to embarrassment, especially if those photos were not intended for public viewing. This situation could make them feel ashamed or hesitant to interact with others.

A respondent said that she concerns about the freedom to live in dignity, highlighting vulnerabilities based on gender and disability in the context of digital threats. She observed that women often seem to be the victims of hacking and fraud, possibly due to perpetrators assuming women are easier to deceive. This perception suggests a gender-based disparity in perceived digital literacy and vulnerability. Additionally, she expressed awareness of the challenges faced by disabled individuals, who may not be as technologically savvy and could require assistance for online activities, raising fears of data misuse. Not all disabled individuals are vulnerable; many are quite capable of protecting their data. However, she feels there are barriers to effectively safeguarding privacy and the social impact of such vulnerabilities, along with the stigma that people with disabilities are weak and easily manipulated in cases of hacking or fraud.

Two other respondents expressed concerns about their freedom to live in dignity in the face of digital security threats, emphasizing the fear of personal data being misused for malicious purposes. A 27-year-old male with a bachelor's degree awaiting job interview calls, shared his fear of financial harm due to responsibilities, after his data was potentially compromised for use by strangers. Despite consulting friends knowledgeable in cyber security, he did not approach any specific institutions for help. Similarly, a 25-year-old male high school graduate working as a freelance game tester, mentioned he has not reported his concerns due to a lack of knowledge on how to do so and prioritizing other matters, fearing that the situation might worsen over time. Both individuals highlight the anxiety and potential impact on men's financial responsibilities and the challenges in seeking recourse or protection against digital threats, underscoring the importance of safeguarding the right to a dignified life free from the exploitation of personal vulner-

https://doi.org/10.22225/.politicos.4.1.2024.56-65

abilities.

Discussion

This section combines the findings from respondents with insights from experts in the digital realm, including those from the Department of Communication and Information Technology of Yogyakarta (DISKOMINFO DIY) and Sleman (DISKOMINFO Sleman), digital security practitioners, and the Jogja Cyber Security Community (JCS). It aims to provide a comprehensive understanding of the discussed topics. In this study, the authors observe that in the case of Bjorka, digital security is part of human security, reflecting a sense of safety and freedom from threats such as hacking that directly affect individuals. A situation can be considered safe when humans possess three freedoms that are core to human security. Freedom is literally the essence of humanity; individuals who experience freedom tend to be active in creating their identities and self-concept. With freedom, humans can control the course of their lives, choose their desired paths, and give meaning to the realities they face (Yunus, 2011).

For the freedom from fear, we are revisiting the context of human security within digital security, the threats encompass not only hacking or exploitation of digital technology and infrastructure for criminal purposes, such as data theft, but also the capacity and interests of digital actors to instigate violence through the construction and incitement of social unrest, violence, and terror, which are further consequences of linguistic constructs within the digital infrastructure (Rachman & Susan, 2021). The respondents' statement in the freedom from fear part demonstrates that the language construction used by the perpetrator, such as provocation, threats, or intimidation, physically affects individuals confronted with it. Language construction conveys information that individuals will respond to. Thus, it is evident that the perpetrator justifies any means to achieve their desired ends (Da Rato & Ardini, 2023).

Facing digital threats, society is required to understand the importance of personal data protection and security aspects in online activities (Zaelany & Putranti, 2023). Personal data protection is crucial in minimizing fear of potential digital crime risks that can undermine individual freedom and civil rights. Digital crimes are part of the transition from manual processes to online systems and the use of communication networks, exploiting public ignorance, which generates fear and anxiety (Sila & Taufik, 2023). The fear arising from internet crimes, known as cyberphobia, directly impacts physically, including worries about pressing the wrong button, anxiety about the social impacts generated by digital media in the community, and fear of personal failure (Aurelya, 2021).

In addressing the concept of freedom from fear, the insights from Mr. Nor Ahmad, founder of Jogja Cyber Security (JCS) and a Cyber Security Analyst at GMEDIAis crucial. He highlights the importance of individuals taking proactive steps in protecting their data, such as employing strong passwords and being cautious about sharing personal information online. This emphasis on personal responsibility in data protection, along with their work in identifying and reporting system vulnerabilities, directly contributes to safeguarding individuals from the fear of cybercrimes and hacking. Meanwhile, Mr. Wahyu Bimo, a technical staff member at the DISKOMINFO Sleman Data Center and founder of the Ngerumpi Security Community, recommends security measures like Two Factor Authentication (2FA) to enhance individual data security.

In terms of freedom from want, the two male respondents in the freedom from want's part, students living away from home, were convinced that the incidents they experienced were Bjorka's doing. Their predicaments stemmed from fabricated origins of wealth or false testimonials designed to attract victims while evading hacking and fraud charges (Sahubawa, Hehanussa, & Hattu, 2023). As a result of these crimes, they suffered financial losses crucial for their daily living as students. The third respondent mentioned that her mother's personal data might have been stolen and misused by others for illicit activities. From the information provided, digital security threats like hacking attacks, malware, and identity theft, as perpetrated by Bjorka, have implications not just for individuals and organizations but for society at large. Digital security is not merely about protecting systems (Kalbu, 2021) but also about ensuring the safety and integrity of hu-

mans within an increasingly interconnected technological ecosystem (Kalalo, 2010). With thorough understanding and appropriate preventive measures, digital security can serve as a foundation for protecting human rights in the evolving digital world (Ginanjar, Firdausyi, Suswandy, & Andini, 2022). This perspective on human security suggests that a safe environment is not only free from fear but also free from want.

Additional discussion is provided by Mrs. Restia Moegiono, an active digital literacy advocate, and Mr. Alfrizal Fakhri from the Security Operation Center of DISKOMINFO DIY. Mrs. Moegiono emphasizes the importance of digital education and self-protection against phishing and other cyberattacks, advocating for increased digital literacy as a means to fulfill the daily needs and rights of individuals, thus aligning with the concept of freedom from want. Furthermore, to communicate digital literacy to the public, Mr. Fakhri suggests conducting more efforts to reach all community layers with education on digital literacy to protect individuals from digital threats and misinformation.

In the freedom to live in dignity, The concept is deeply intertwined with the ability of individuals to navigate and understand digital life, emphasizing the fundamental human right to a life of dignity, honor, and quality, safeguarded against any threats that might undermine one's sense of self-worth. The digital era brings with it challenges that require a comprehensive understanding of digital security and privacy to maintain one's dignity in an increasingly interconnected world (Tadjbakhsh, 2014; Komnasham.go.id, n.d.). This perspective is crucial in recognizing and combating the digital divide that can exacerbate existing inequalities and vulnerabilities. Moreover, the discussion extends to the significant challenges faced by individuals with disabilities in the digital realm, spotlighting issues of ableism where discrimination and stereotypes can hinder their full participation in digital activities.

This reveals a broader societal issue where the lack of digital accessibility and understanding can lead to exclusion and undermine the dignity of those with disabilities. It's imperative, as noted by Sitorus (2023), Amnesty International Indonesia (2023), and Pathak (2014) to ensure equitable digital rights and opportunities for all, fostering an environment where everyone can achieve well-being and success, free from discrimination or prejudice, in alignment with broader human security goals. The feedback from respondents reinforces the inviolability of human dignity, extending this principle to cyberspace, which ought to be a safe and inclusive space for contribution and interaction. This underscores the importance of digital dignity, advocating for a cyberspace that respects and upholds human dignity, enabling every individual to engage confidently and securely (Digital Dignity, n.d.). As we navigate the complexities of the digital age, it becomes clear that ensuring dignity in digital interactions is not just about protecting data, but about fostering a culture of respect, inclusion, and empowerment for all users, regardless of their backgrounds or abilities.

The cyber experts, Mr. Fakhri and Mrs. Moegiono, emphasis on inclusive digital education programs, particularly for persons with disabilities and other vulnerable groups. Their acknowledgment of the challenges faced by certain communities in accessing online training or literacy and the call for more comprehensive digital education initiatives reflect a commitment to ensuring that everyone has the right to participate fully and safely in the digital world. This approach not only aims to protect individuals from digital threats but also to empower them to engage confidently and securely in cyberspace, thereby supporting the freedom to live with dignity in the digital age.

Conclusion

In the digital era, particularly in relation to the hacking incidents by Bjorka, digital security has become an integral aspect of human security, reflecting a sense of safety and freedom from threats such as hacking. Bjorka utilized social media to disseminate hacked data, highlighting the complexity of digital security, which is not only a technical issue but also related to human rights. Responses to digital insecurity are also influenced by gender identity, indicating that digital security issues involve broader dimensions. A situation can be considered secure when humans possess three freedoms that are core to human security. Freedom is literally the essence of humanity;

https://doi.org/10.22225/.politicos.4.1.2024.56-65

individuals who experience freedom tend to be active in creating their identities and self-concept. With freedom, humans can control the course of their lives, choose their desired paths, and give meaning to the realities they face (Yunus, 2011). The presence of freedom motivates humans to be the principal architects in shaping their lives and the meaning of their experiences. Therefore, human security has three main components: freedom from fear, freedom from want, and freedom to live in dignity. These emerge as guidelines to affirm the realization of a safe environment from threats as fundamental rights that must be fulfilled.

The relationship between the concept of human security, which then evolved with the advent of digital security, lies in the importance of protecting human rights in the digital world. Digital security involves not only the protection of personal data and technology security but also aspects of human rights. For example, the right to privacy is part of freedom from fear in the digital context. The protection of personal data is key to avoiding the misuse of information that can threaten an individual's physical privacy. In addition, aspects of social welfare such as equal access to information and technology play a role in achieving freedom from want in the digital era. Equal and fair access to digital technology forms the basis for overall human security, ensuring that digital life also reflects these human rights principles. Meanwhile, freedom to live in dignity, for example, includes the freedom of expression without interference or threats that can damage an individual's dignity.

This research underscores the crucial role of governments in focusing on human security. Equal data protection becomes a primary focus to prevent disruptions in community life due to digital insecurity. With responsive and robust policies, it is hoped that fundamental individual rights can be preserved, and society remains protected from potential threats. The Bjorka case also reflects inequalities in digital access and understanding of data security. Equal and fair access to digital technology is considered foundational for overall human security. Therefore, policies that ensure digital security and address access gaps need to be strengthened. Involving individuals as primary rights holders and considering gender dimensions in responses to digital insecurity are important steps towards achieving inclusive and holistic human security.

References

Alkire, S. (2003). *A conceptual framework for Human Security*. Centre for Research on Inequality, Human Security, and Ethnicity, CRISE.

Amnesty International Indonesia (2023). Standar hidup layak. *Amnesty.id*. Accessed on November 7th, 2023, from https://www.amnesty.id/standar-hidup layak/#:~:text=Hidup% 20bermartabat%20berarti%20setiap%20orang,atas%20air%20bersih%20dan%20sanitasi

Anantaka, H., G., Zulfa, E., A., & Nita, S. (2023). Bjorka: A cyber crime phenomenon which gets support from the community using analysis of criminological perspective. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, *6*(2), 1120-1129.

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 5*(1), 95-110.

Arif, F. M., & Chania M., S. (2022). Aktualisasi standar penalaran filosofis dalam perlindungan data pribadi. *Jurnal Studi Islam, 11* (1), 1-25.

Aurelya, C. H. (2021). Pengaruh intensitas penggunaan media sosial terhadap munculnya sindrom fear of missing out (FOMO) (Studi Kasus Media Sosial TikTok di Kalangan Generasi Z) (Doctoral dissertation, Universitas Atma Jaya Yogyakarta).

Bachtiar, P., P., Diningrat, R. A., Kusuma, A. Z. D., Izzati, R. A., & Diandra, A. (2020). *Ekonomi digital untuk siapa? Menuju ekonomi digital yang inklusif di Indonesia*. Smeru Research Institute.

Budi, E., Wira, D., & Infantono, A. (2021). *Strategi penguatan cyber security guna mewujudkan keamanan nasional di era society 5.0*. In Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO).

Brown, D. & Esterhuysen, A. (2019). *Why cybersecurity is a human rights issue, and it is time to start treating it like one*. APCNews.

Cahyadi, I. (2018). Tata kelola dunia maya dan ancaman kedaulatan nasional. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *7*(2) 210-232.

Candra, D., S. & Wardoyo, B. (2020). Implementing human security measures in the cyberspace: Navigating through the institutional and regulatory disarray. *IR UI Commentaries*, *1*(9), 1-5.

CNN Indonesia (2022). KPU buka suara soal dugaan 105 Juta data warga Indonesia bocor. *CNN Indonesia.com.* Accessed on October 6th, 2023, from https://www.cnnindonesia.com/nasional/20220906223223-20-844262/kpu-buka-suara-soal-dugaan-105-juta-data-warga-indonesia-bocor

Da Rato, E. Y., & Ardini, L. (2023). Pengaruh Fraud Triangle terhadap kecenderungan Fraud Anggaran Dana Desa dan budaya organisasi sebagai Variabel Moderasi: (Studi pada Pemerintah Desa di Kabupaten Sikka). *Riset dan Jurnal Akuntansi, 7*(4), 3433-3446.

Digital Dignity (n.d.). Our intended impact. *digital.dignity lab*. Accessed on November 8th, 2023 from https://digitaldignity.io/en

Farhan A., & Cindy (2023). Perlindungan hukum data pribadi di Indonesia. *Prosiding Seminar Nasional Hasil Penelitian dan Pengabdian kepada Masyarakat (SINAPENMAS)*, *2*(1), 947-951. Universitas Tarumanegara.

Gani, T. A. (2023). *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press.

Gasper, D., & Gómez, O. A. (2015). Human security thinking in practice: Personal security, citizen security and comprehensive mappings*. Contemporary Politics*, *21*(1), 100–116.

Ginanjar, D., Firdausyi, M., F., Suswandy, S., & Andini, N., T. (2022). Perlindungan HAM dalam era digital: Tantangan dan solusi hukum. *Journal on Education, 4* (4), 2080-2094.

Gustiana, A. (2022). Bukti Hacker Bjorka berasal dari Indonesia. *Bandung.viva.co.id*. Accessed on October 5th, 2023, from https://bandung.viva.co.id/news/7353-bukti-hacker-bjorka-berasal-dari-indonesia

Halimawan, A., Hardenta, A.D., Hayati A., N., Indradi, A., H., Arsyah, A., M., Mulyani, C., K., Athilla, K., D., Faruq, M., H., A., Rayhan, M., Aldebarant, N., R., R., Puspitarasi, S., Pangestu, T., H., & Incusy, T., R. (2020). *Mencari solusi permasalahan instrumen hukum perlindungan data pribadi di Indonesia*. Kajian Dewan Mahasiswa Justisia Fakultas Hukum Universitas Gadjah Mada.

Hardiansyah, Z. (2022). Apa itu Breached Forums yang terlibat 4 kasus kebocoran data di Indonesia sebulan terakhir? *Kompas.com.* Accessed on October 6th, 2023, from https://tekno.kompas.com/read/2022/09/07/16150067/apa-itu-breached-forums-yang-terlibat-4-kasus-kebocoran-data-di-indonesia?page=all

Hidayat, R., A. (2017). Keamanan Manusia dalam perspektif studi Keamanan Kritis terkait perang intra-negara. *INTERMESTIC Journal of International Studies, 1*(2), 108-129.

Indah, F., Sidabutar, A. Q., & Nasution, N. A. (2022). Peran cyber security terhadap keamanan data penduduk negara Indonesia (Studi kasus: Hacker Bjorka). *Jurnal Bidang Penelitian Informatika*, *1*(1), 1-8.

Kalalo, H. (2010). Kesehatan dan unjuk kerja ekosistem teknologi informasi. *Journal of Business and Economics, 9* (2), 156-160.

Kalbu, T., I. (2021). Keamanan Digital lebih dari sekadar mengamankan perangkat. *Kompas.id*. Accessed on November 7th, 2023, from https://adv.kompas.id/baca/keamanan-digital-lebih-dari-sekadar-mengamankan-perangkat/

Klein, J., & Hossain, K. (2020). Conceptualising human-centric cyber security in the arctic in light of digitalisation and climate change. *Arctic Review on Law and Politics*, *11*, 1-18. https://www.jstor.org/stable/48710620

Komnasham.go.id (n.d.). Deklarasi Universal Hak Asasi Manusia. *Komnasham.go.id*. Accessed on November 8th, 2023, from https://www.komnasham.go.id/files/1475231326-deklarasi-universal-hak-asasi--$R48R63.pdf

Kurnia, R. (2023). *The rise of hacktivism and emerging issues in data protection in Indonesia*. Accessed on November 8th, 2023, from https://www.researchgate.net/profile/Rifan-Kurnia/publication/368544433_The_Rise_of_Hacktivism_and_Emerging_Issues_in_Data_Protection_in_Indonesia/links/63ee005f2958d64a5cd5ab4e/The-Rise-of-Hacktivism-and-Emerging-Issues-in-Data-Protection-in-Indonesia.pdf

Lauermann, J. (2022). Dignity, mega-projects, and the problem of scale. *Dialogues in Human Geography*, *12* (3), 431-435.

Pathak, B. (2014). Human Security and Human Rights: Harmonious to inharmonious relations. *Archives of Business Research, 2*(1), 46-74.

Peraturan Perundang-undangan Pemerintah Republik Indonesia (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Putsanra, D., V. (2022). Arti nama Bjorka dan update terkini kebocoran data Kominfo. *Tirto.id.* Accessed on October 5th, 2023, from https://tirto.id/arti-nama-bjorka-dan-update-terkini-kebocoran-data-kominfo-gv9F

Rachman, M., F. & Susan, N. (2021). Modal sosial masyarakat digital dalam diskursus keamanan siber. *Jurnal Indonesia Maju*, *1*(1), 1-11.

Ridwan, P., P. (2022). Mengukur provinsi paling gaptek di Indonesia. *Goodstats.id.* Accessed on September 27th, 2023, from https://goodstats.id/article/mengukur-provinsi-paling-gaptek-sebagai-bukti-ketimpangan-R0ugb

Sahubawa, M., A., Hehanussa, D., J., A., & Hattu, J. (2023). Penipuan berkedok investasi jenis Binary Option. *PATTIMURA Law Study Review, 1*(1), 146-153.

Saptohutomo, A., P. (2023). Pakar ungkap data paspor dibocorkan peretas Bjorka valid. *Kompas.com.* Accessed on September 4th, 2023, from https://nasional.kompas.com/read/2023/07/07/16003551/pakar-ungkap-data-paspor-dibocorkan-peretas-bjorka-valid

Shiba, N. (2022). Sejumlah aksi pembobolan data oleh Bjorka, apa bahayanya? *Ids.ac.id*. Accessed on October 6th, 2023, from https://ids.ac.id/aksi-pembobolan-data-oleh-bjorka/

Siahaan, N., H., T. (2004). *Hukum lingkungan dan ekologi pembangunan*. Erlangga.

Sila, G. E., & Taufik, C. M. (2023). Literasi digital untuk melindungi masyarakat dari kejahatan siber. *KOMVERSAL, 5*(1), 112-123.

Sitorus, N. G. (2023). Dari "Ableist" menuju "Dis-ableist": Membangun Gereja yang inklusiv bagi penyandang disabilitas. *Jurnal Teologi Cultivation*, *7*(1), 31-45.

Soewardi, B. A. (2013). *Perlunya pembangunan sistem pertahanan siber (cyber defense) yang tangguh bagi Indonesia*. Media Informasi Ditjen Pothan Menhan.

Solove, D., J., & Citron, D., K. (2017). Risk and anxiety: A theory of data-breach harms. *Texas Law and Review*, *96*(4), 737-786.

Sukmawan, D. I., & Setyawan, D. P. (2023). Hacker, fear, and harm: Data breaches and national security. *Global Strategis, 17* (1), 153–182. https://doi.org/10.20473/jgs.17.1.2023.153-182

Sumiati, E., & Wijonarko, W. (2020). Manfaat literasi digital bagi masyarakat dan sektor pendidikan pada saat pandemi Covid-19. *Buletin Perpustakaan Universitas Islam Indonesia, 3*(2), 65-80.

Tadjbakhsh, S. (2014). *Human security twenty years on*. Norwegian Peacebuilding Resource Center.

UNDP (1994). *New dimension of human security*. United Nations Development Programme.

Wardoyo, B. (2015). *Perkembangan, paradigma, dan konsep keamanan internasional dan relevansinya untuk Indonesia*. Nugraha Media.

Yunus, F. M. (2011). Kebebasan dalam Filsafat Eksistensialisme Jean Paul Sartre. *Al-Ulum, 11* (2), 267-282.

Zaelany, A., F., & Putranti, I., R. (2023). Pelanggaran privasi dan ancaman terhadap Keamanan Manusia dalam kasus Cambridge Analytica. *Journal of International Relations, 9* (1), 125-137.