Zaky Anggara, *et al.*
Al Hurriyah : Jurnal Hukum Islam
http://dx.doi.org/10.30983/al-hurriyah.v11i1.10837

Al-Hurriyah : Jurnal Hukum Islam
e-ISSN: 2549-4198 - p-ISSN: 2549-3809
Vol. 11. No. 1. Edition June 2026

ORIGINAL ARTICLE OPEN ACCES

BJORKA'S CYBERCRIMES FROM THE PERSPECTIVE OF *FIQH JINAYAH*

Zaky Anggara[1*], Mohamad Sar'an[2], Enceng Arif Faizal[3], Muhammad Akbar Khan[4]

***Corespondence :**
Email : zakyanggarastudent@gmail.com

Affiliation:
[1, 2, 3] Universitas Islam Negeri Sunan Gunung Djati Bandung, *Indonesia*
[4] International Islamic University Islamabad, *Pakistan*

Article History :
Submission : December 27, 2025
Revised : February 24, 2026
Accepted : May 28, 2026
Published : June 10, 2026

Keyword : Bjorka Cybercrime, Criminal Liability, Fiqh Jinayah, Islamic Sanctions, Ta'zir Punishment

Abstract

This study aims to analyze Bjorka's cybercrimes from the perspective of Islamic criminal law (*fiqh jināyah*) by examining the concept of criminal liability (*al-mas'ūliyyah al-jinā'iyyah*) and formulating a classification of sanctions (*ʿuqūbāh*) applicable to contemporary cyber offenses. The study employs normative legal research using a descriptive—analytical approach through the examination of primary sources of Islamic law, classical and contemporary *fiqh* literature, statutory regulations, and relevant academic publications, which are analyzed qualitatively to construct a legal framework for addressing cybercrime. The findings reveal that Bjorka's cyber activities constitute *jarīmah taʿzīr* because no explicit textual provisions prescribe specific punishments for hacking and related cyber offenses, although such acts embody prohibited elements of *al-kadhib* (falsehood), *akhdh al-māl bi ghayr ḥaqq* (unlawful appropriation of property), *tajassus* (unauthorized surveillance), and violations of the objectives of Islamic law (*maqāṣid al-sharīʿah*). The study further classifies *taʿzīr* sanctions into light, moderate, and severe categories based on the nature of the offense, the degree of harm, and its impact on individuals, society, and state security. The study concludes that the principles of *fiqh jināyah* provide a flexible normative basis for addressing contemporary cybercrimes through proportional *taʿzīr* sanctions while maintaining justice, deterrence, and public welfare. This research contributes a systematic framework for assessing criminal liability and classifying sanctions for cybercrime within *fiqh jināyah*, thereby strengthening the theoretical development of Islamic criminal law in responding to emerging digital crimes and supporting future cybercrime policy formulation.

Abstrak

Penelitian ini bertujuan untuk menganalisis kejahatan siber yang dilakukan oleh Bjorka dalam perspektif hukum pidana Islam (fiqh jināyah) dengan mengkaji konsep pertanggungjawaban pidana (al-mas'ūliyyah al-jinā'iyyah) serta merumuskan klasifikasi sanksi (ʿuqūbāh) yang dapat diterapkan terhadap tindak pidana siber kontemporer. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan deskriptif-analitis melalui kajian terhadap sumber-sumber primer hukum Islam, literatur fiqh klasik dan kontemporer, peraturan perundang-undangan, serta publikasi ilmiah yang relevan, yang dianalisis secara kualitatif untuk membangun kerangka hukum dalam penanggulangan kejahatan siber. Hasil penelitian menunjukkan bahwa aktivitas siber Bjorka termasuk dalam kategori jarīmah taʿzīr karena tidak terdapat ketentuan nash yang secara eksplisit menetapkan sanksi terhadap peretasan dan tindak pidana siber sejenis. Namun, perbuatan tersebut mengandung unsur al-kadhib (kebohongan), akhdh al-māl bi ghayr ḥaqq (pengambilan harta tanpa hak), tajassus (spionase atau penyadapan tanpa hak), serta bertentangan dengan tujuan syariat Islam (maqāṣid al-sharīʿah). Penelitian ini juga mengklasifikasikan sanksi taʿzīr ke dalam kategori ringan, sedang, dan berat berdasarkan karakteristik perbuatan, tingkat kerugian yang ditimbulkan, serta dampaknya terhadap individu, masyarakat, dan keamanan negara. Penelitian ini menyimpulkan bahwa prinsip-prinsip fiqh jināyah menyediakan landasan normatif yang fleksibel untuk menangani kejahatan siber kontemporer

melalui penerapan sanksi ta'zīr yang proporsional dengan tetap menjunjung nilai keadilan, efek jera, dan kemaslahatan umum. Kontribusi akademik penelitian ini terletak pada perumusan kerangka sistematis mengenai pertanggungjawaban pidana dan klasifikasi sanksi terhadap kejahatan siber dalam perspektif fiqh jināyah, sehingga memperkaya pengembangan teori hukum pidana Islam dalam merespons kejahatan digital serta menjadi landasan normatif bagi pengembangan kebijakan penanggulangan kejahatan siber di masa mendatang.

INTRDUCTION

The development of digital technology has driven a transformation in criminal patterns from conventional forms towards cybercrime, which is becoming increasingly complex and has far—reaching implications for national security, social stability, data protection and individual interests.[1] However, these developments are often not matched by the capacity of positive law to respond to new criminal methods, which evolve more rapidly than the formulation of regulations.[2] This situation reflects the gap between law in the books and law in action as articulated by Roscoe Pound,[3] particularly in the context of applying the principle of *nullum delictum nulla poena sine praevia lege poenali* (there can be no crime and no punishment without a pre—existing criminal law), which results in the law tending to be reactive to the dynamics of cybercrime.

In Indonesia, regulations concerning cybercrime have been established through Law No. 11 of 2008 on Electronic Information and Transactions, as amended, and Law No. 27 of 2022 on Personal Data Protection. Nevertheless, the implementation of these regulations still faces various challenges, such as ambiguous provisions, multiple interpretations,[4] and delays in adapting to technological developments.[5] Data from the Badan Siber dan Sandi Negara (BSSN) indicates a high incidence of data breaches, website defacement, phishing, and *Advanced Persistent Threat* (APT) targeting various sectors in Indonesia.[6] This situation has been further exacerbated by data leaks linked to Bjorka, an anonymous cyber actor known for alleged hacking and the dissemination of government data and the personal data of Indonesian citizens in 2022—2023, which highlights the weakness of digital defences, law enforcement, and government transparency.[7] The Ministry of

[1] Shuai Chen et al., "Exploring the Global Geography of Cybercrime and Its Driving Forces," *Humanities And Social Sciences Communications* 10, no. 71 (2023): 1—10, https://doi.org/10.1057/s41599—023—01560—x.

[2] Rhaysya Admmi Habibani, Siti Fatimah, and Azmi Fitrisia, "Positivisme: Konsep, Perkembangan, Dan Implementasi Dalam Kajian Ilmu Pengetahuan Dan Hukum," *Cendekia: Jurnal Ilmu Pengetahuan* 4, no. 4 (2024): 524—32, https://doi.org/10.51878/cendekia.v4i4.3831.

[3] Pandam Bayu Seto Aji and Zain Arfin Utama, "Hukum Sebagai Kenyataan: Teori Sebagai Objek Studi Dan Bahan Penelitian," *Al-Zayn* 3, no. 2 (2025): 3682—83, https://doi.org/10.61104/alz.v3i4.1579.

[4] I wayan Pastika, Eirenne Pridari Sinsya Dewi, and Ida Bagus Gede Dharma Putra, "Language Cases Against UU ITE in Indonesia," *International Journal of Linguistics, Literature and Culture* 9, no. 5 (2023): 198—208, https://doi.org/10.21744/ijllc.v9n5.2361.

[5] Astri Aprilianti, "Efektivitas Dan Implementasi Undang—Undang Informasi Dan Transaksi Elektronik Sebagai Hukum Siberdi Indonesia: Tantangan Dan Solusi," *Begawan Abioso* 15, no. 1 (2024): 41—50, https://doi.org/10.37893/abioso.v15i1.1002.

[6] Badan Siber Dan Sandi Negara, "Cybersecurity Monitoring Report 2020 Dan 2021," *Biro Hukum Dan Komunikasi Publik — BSSN*, 2021.

[7] Safrida Nurulita and Ridwan, "Political Will Of The Indonesian Government In Addressing Data Leakage And Cybersecurity In The Era Of Digital Transformation," *Jhss*

Communication and Information Technology (KOMINFO) believes that this phenomenon reflects the fragility of the digital security system as well as the ineffectiveness of cyber law enforcement in Indonesia.[8]

Islamic criminal law, or *fiqh jināyah*, consistently offers epistemological remedies based on *maṣlaḥatiyyah* (public interest) that are more compatible with the dynamics of modern technology, as they are oriented towards the protection and welfare of the community.[9] The paradigm that asserts that Islamic criminal law is incompatible with modernity reflects a failure to interpret sharia as a legal system with a moral and philosophical foundation that is flexible in addressing the dynamics of the times. In truth, Islam has never rejected progress, but rather guides it to remain within the framework of Sharia values, as argued by Muhammad Abed Al—Jabiri through burhani reasoning (a system of rational thought and critical analysis), so that the law may be understood contextually and remain relevant to the developments and needs of modern society.[10] The principle of *Jalb al-Maṣāliḥ wa Dafʿ al-Mafāsid* affirms that the primary objective of Islamic Sharia is to seek benefit and avert harm, as emphasised by al—Shaṭibi, who stated that the primary objective of Sharia is to safeguard the public interest.[11] Within the Islamic worldview, cybercrime is viewed not merely as a legal violation, but also as a sinful act that undermines the principles of *ʻadl* (justice), *amanah* (trust), and *masʻuliyyah* (accountability). [12] Bjorka's actions have violated the objectives of Islamic law, such as the principles of *ḥifẓ al-ʻaql* (protection of the mind), *ḥifẓ al-māl* (protection of property), and *ḥifẓ al-ʻird* (preservation of honour) within the framework of *maqāṣhid al-syarīʻah*.

A number of previous studies have examined the Bjorka phenomenon from various perspectives, but have not yet provided a formulation of criminal liability or a concept of sanctions that is both operational and applicable. The study by Achmad Fageh and Anisa Solikhawati entitled, "*The Bjorka Hacking Phenomenon on Selling Personal Data as a Digital Asset from The Perspective of Maqāṣhid Sharia*" focuses on violations of the principles of *maqāṣhid al-syarīʻah*, particularly *ḥifẓ al-māl*, by treating personal data as a form of digital asset within the framework of *fiqh muammalah*. Nevertheless, the study places greater emphasis on the normative ethical dimension and the protection of digital assets, and thus has not yet elaborated on the form of criminal liability for Bjorka's

(Journal Of Humanities And Social Studies) 9, no. 1 (2025): 28—38, https://doi.org/10.33751/jhss.v9i1.33.

[8] Mansur Juned, Ali Martin, and Nugraha Pratama, "Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity," *Academic Journal of Interdisciplinary Studies* 13, no. 5 (2024): 369—80, https://doi.org/10.36941/ajis—2024—0171.

[9] Fitri Wahyuni, *Hukum Pidana Islam: Akulturasi Nilai-Nilai Hukum Pidana Islam Dalam Pembaharuan Hukum Pidana Indonesia* (Tangerang Selatan: PT Nusantara Persada Utama, 2018), p.1—3.

[10] Lina Nur Anisa, "Reformasi Hukum Pidana Islam: Telaah Nalar Arab Muhammad Abed Al—Jabiri," *Journal of Islamic Economic and Law (JIEL)* 2, no. 1 (2025): 1—19, https://doi.org/10.59966/jiel.v2i1.1523.

[11] Muh. Ilham Azis et al., 'Maqasid Al—Shari'ah Theory By Imam Al—Syatibī', *Anayasa : Journal of Legal Studies* 2, no. 1 (2024): 17—34, https://doi.org/10.61397/ays.v2i1.191.

[12] Kalil Alfazari, Mohamad Azrien Mohamed Adnan, and Tengku Sarinja Aini Tengku Kasim, "Cybercrime in Contemporary Society: An Islamic Worldview on Its Framework, Motivations, and Consequences," *Journal of Islamic Educational Research* 11, no. 1 (2025): 46—62, https://doi.org/10.22452/jier.vol11no1.5.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

cybercrimes.[13] Meanwhile, the research by Radika Hanny Syah and her colleagues, in their research paper, *"Analisis Keamanan Siber dan Hukum: Studi Kasus Bjorka"* discusses Bjorka's modus operandi from the perspective of cybersecurity and Indonesian positive law, specifically the ITE Law and personal data protection regulations. The limitation of this research lies in its predominantly technical—legal approach, which has not yet addressed the philosophical foundations of criminal liability nor touched upon the values of *fiqh jināyah* in relation to the development of modern cybercrimes.[14] Yuko Fitrian's research entitled, *"Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara"* has even classified Bjorka's actions as a form of cyber—terrorism, yet its primary focus remains on classification and criminal penalties under national law, without addressing the more fundamental question of the perpetrator's liability.[15] Unlike previous research, which has focused on the protection of digital assets from the perspective of *maqāṣhid al-syarī'ah*, cybersecurity, or the classification of Bjorka's actions as cyber—terrorism under positive law, this article examines Bjorka's criminal acts from the perspective of *fiqh jināyah*, with an emphasis on the formulation of criminal liability and the concept of sanctions appropriate to the characteristics of contemporary cybercrime. Its novelty lies in the development of the construction of *al-mas'uliyyah al-jinā'iyyah*, the classification of *'uqūbah* (sanctions), as well as operational parameters and indicators that can be applied contextually to the dynamics of modern cybercrime. These findings are relevant for the development of cyber criminal law in Indonesia that is more adaptive, proportionate, and oriented towards the public interest.

Given this research gap, this article aims to address two main issues. Firstly, how is the *al-mas'uliyyah al-jinā'iyyah* (criminal liability) of the perpetrator of Bjorka's cybercrime determined under Islamic criminal law? Secondly, how does the concept of *'uqūbah* (punishment) apply to Bjorka's cybercrime when viewed through the principles of Islamic criminal law? These two issues are important to examine given that the complexity of cybercrime continues to give rise to new forms of offences that cannot always be adequately addressed through conventional legal approaches. The novelty of this research lies in criminal liability with operational parameters and the imposition of measurable sanctions through sentencing indicators, so that it does not remain at a normative—theological level, but is relevant to the needs of state law enforcement and the protection of the public interest. Thus, the contribution of this research not only fills a gap in the study of *fiqh jināyah* regarding cyber offences, but also offers a conceptual foundation for the development of a cyber sentencing approach within national law that is more responsive to the complexity of digital crime. This research aims to formulate a model of criminal liability and a concept of punishment based on *fiqh jināyah* that is relevant to cybercrimes such as the Bjorka case.

[13] Achmad Fageh and Anisa Solikhawati, "The Bjorka Hacking Phenomenon on Selling Personal Data as a Digital Asset from The Perspective of Maqashid Sharia," *Jurnal Hukum Islam* 20, no. 2 (2022): 279—354, https://doi.org/10.28918/jhi.v20i2.6387.

[14] Radika Hanny Syah and Muhammad Irwan Padli Nasution, "Analisis Keamanan Siber Dan Hukum: Studi Kasus Bjorka," *Jurnal Ilmiah Ekonomi, Manajemen, Bisnis Dan Akuntansi* 2, no. 3 (2025): 329—338, https://doi.org/10.61722/jemba.v2i3.948.

[15] Yuko Fitrian, "Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka Terhadap Data Negara," *Arus Jurnal Sosial Dan Humaniora* 3, no. 3 (2023): 164—74, https://doi.org/10.57250/ajsh.v3i3.278.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

METHODS

This study employs a normative legal approach (doctrinal legal research) using descriptive—analytical methods through a conceptual approach and a comparative approach. The conceptual approach is used to analyse and construct the concept of *al-mas'uliyyah al-jinā'iyyah* (criminal liability) and the classification of *ʿuqūbāh* (sanctions) in *fiqh jināyah* in relation to the phenomenon of contemporary cybercrime, particularly the Bjorka case, which is not explicitly regulated in classical Islamic legal sources. Meanwhile, the comparative approach is used to compare the construction of criminal liability and the classification of sanctions between Indonesian positive law and Islamic criminal law in responding to cybercrime. The data used consists of secondary qualitative data obtained through a literature review of primary legal sources, including the Qur'an, Hadith, relevant legislation such as the ITE Law and the PDP Law, as well as classical (*turāth*) and contemporary literature, whilst secondary legal materials include books, academic articles, and data from the Badan Siber dan Sandi Negara (BSSN) relevant to the research topic. Data collection was carried out through the identification and selection of various sources relating to criminal liability, the elements of cybercrimes, and the concept of sanctions in Islamic criminal law. Data analysis was conducted in stages through an interpretation of the concepts of *al-mas'uliyyah al-jinā'iyyah*, *jarīmah*, and *ʿuqūbāh*, the identification of criminal elements in the Bjorka case, a comparison of legal frameworks between positive law and *fiqh jināyah*, the classification of offences based on *fiqh jināyah* categories, and the systematisation of the analysis results to formulate a framework for criminal liability and a model of sanctions for cybercrime based on the principles of *maqāṣid al-syarī'ah*, thereby producing a conceptual formulation relevant to the development of modern cybercrime.

RESULT AND DISCUSSION

RESULT

The Criminal Liability of the Cybercriminal Bjorka under Islamic Criminal Law

Islamic criminal law or *fiqh jināyah*, is a branch of Islamic law that governs prohibited acts or neglected obligations committed by legally accountable individuals (*mukallaf*); the nature and severity of the penalties are determined in accordance with the provisions of Sharia and aim to uphold justice, protect individual rights, and safeguarding the public interest, as emphasised by the research of Zulkifli Muda and his colleagues.[16] A criminal act in *fiqh jināyah* is called a *jarīmah*; it is an act prohibited by Sharia and subject to sanctions as a consequence of the offence committed.[17] In the context of *fiqh jināyah*, *jarīmah* is classified into three categories: *jarīmah ḥudūd*, *jarīmah qiṣāṣh-diyat*, and *jarīmah ta'zīr*. *Jarīmah ḥudūd* refers to offences where the nature and severity of the punishment for each crime have been explicitly prescribed by Allah SWT specifically in the text. *Qiṣāṣh-diyat* crimes are offences relating to murder and assault, based on the principle of retributive justice and the right of the victim or their family to demand commensurate retribution or to settle the matter through diyat (compensation). Meanwhile, *jarīmah ta'zīr*

[16] Zulkifly Muda, Nizaita Omar, and Nehaluddin Ahmed, "Comparison Between Islamic Criminal Law and Man—Made Law," *Internasional Journal Of Academic Research In Business & Social Sciences* 14, no. 2 (2024): 972—80, https://doi.org/10.6007/IJARBSS/v14—i2/20718.

[17] Muḥammad Abū Zahrah, *Al-Jarīmah Wa Al-'Uqūbah Fī Al-Fiqh Al-Islāmī* (al—Qahirah: Dar al—Fikr al—ʿArabī, 1998), p.17.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

refers to all forms of offences for which the extent of the punishment is not directly specified in the naṣh, so that the determination of the punishment is left to the authority of the ruler or judge based on the principle of the public interest.[18] Cybercrime is clearly a new manifestation of a crime or unlawful act that causes harm to people's minds, property, honour and security.

Bjorka is an anonymous figure known as a cyber actor due to a series of alleged hacks, data leaks and the distribution of both government data and the personal data of Indonesian citizens between 2022 and 2023. Their emergence began to attract public attention from 20 August 2022 after their activities were identified on Breach Forums, a dark web platform frequently used as a space for the distribution and trading of hacked data.[19] Bjorka subsequently claimed to possess and disseminate various strategic data, including SIM card registration data, digital service customer data, and information linked to government institutions.[20] This phenomenon not only highlights the high vulnerability of the national digital security system but has also sparked debate regarding the effectiveness of data protection regulations and the capacity of cyber law enforcement in Indonesia. Furthermore, Bjorka's activities represent a shift in criminal patterns towards modern forms of cybercrime that exploit technological advancements to gain illegal access to electronic data, thereby impacting privacy protection, national security, and public trust in digital governance. According to various academic sources, Bjorka's activities can be categorised as a form of cybercrime with specific characteristics and patterns of infringement that reflect the complexity of contemporary cybercrime modus operandi, as outlined in the following details:

Table 1. Analysis of Cybercrime Cases by Bjorka

Types of Crime	Evidence and Data Validity	Alleged Status
Doxing public officials	Bjorka's Twitter and Telegram posts sharing data on public officials (Jhonny G. Plate, Puan Maharani, Erick Thohir, etc.)[21]	Confirmed by the public and the media
Threats against Pertamina	A post threatening to release Pertamina's database[22]	It's just a threat
IndiHome data breach (26 million search histories)	The breached.to forum claims there has been an Indihome data breach (domains, keywords, IP addresses, email addresses, etc.)[23]	Telkom has disputed the validity of the data

[18] Hajed A. Altaibi, "The Challenges of Execution of Islamic Criminallaw in Developing Muslim Countries: An Analysisbased on Islamic Principles and Existing Legalsystem," *Law, Cogent Social Sciences* 7, no. 1 (2021): 1–13, https://doi.org/10.1080/23311886.2021.1925413.

[19] Inayah Fasawwa Putri and Moody Rizqy Syailendra Putra, "Criminal Liability of Perpetrators of Sim Card Registration Data Hacking Under the Eit Law and The PDP Law," *Awang Long Law Review* 8, no. 1 (2025): 212–22, https://doi.org/10.56301/awl.v8i1.1909.

[20] M Jacky and FX Sri Sadewo, "Indonesian Blogger Analyzing Bjorka Hacker," *Technium Social Sciences Journal* 50, no. special issue (2023): 532–542, https://doi.org/10.47577/tssj.v50i1.9937.

[21] Jacky and Sadewo.

[22] Tole Sutikno and Deris Stiawan, "Cyberattacks and Data Breaches in Indonesia by Bjorka: Hacker or Data Collector?," *Bulletin of Electrical Engineering and Informatics* 11, no. 6 (2022): 2989–94, https://doi.org/10.11591/eei.v11i6.4854.

[23] Annisa Nadya Putri, "Upaya Hukum Dalam Strategi Perlindungan Data Pada Penggunaan Internet Studi Kasus : Hacker Bjorka," *Jurnal Hukum Dan Pembangunan Ekonomi* 12, no. 1 (2024): 52–64, https://doi.org/10.20961/hpe.v12i1.81910.

Types of Crime	Evidence and Data Validity	Alleged Status
Doxing public officials	Bjorka's Twitter and Telegram posts sharing data on public officials (Jhonny G. Plate, Puan Maharani, Erick Thohir, etc.)[21]	Confirmed by the public and the media
Sale of SIM card registration data (1.3 billion records)	Breached forums, screenshot evidence[24]	Some have been validated by security expert Tanujaya
KPU data breach (105 million records of residents)	The breached.to forum claims to have hacked the KPU database[25]	The KPU has not yet confirmed the leak
Claims regarding classified documents from the President and the National Intelligence Agency	Claims of possessing letters from the BIN (Badan Intelijen Negara) and the President on the breached.to forum[26]	Denied by the President's Secretariat
MyPertamina data breach (44 million records)	MyPertamina data on a dark web forum, linked to the subsidised fuel registration system[27]	A user data breach has been identified

***Sources**: The data was processed by the researchers*

Criminal liability or *al-mas'uliyyah al-jinā'iyyah*, within Islamic legal tradition is influenced by various theological approaches, such as the *Ash'ari* school of thought, which this study positions as the most moderate approach between the determinism of the *Jabariyah school* and the rationalism of the *Mu'tazilah school*. According to the *Ash'ari school*, humans possess the ability to choose and perform actions (*af'āl ikhtiyāriyyah*), that is, acts stemming from the will, although this ability is, in essence, created by Allah.[28] Thus, humans retain a sphere of free will which forms the basis for the attribution of responsibility for an action. This framework is reinforced by the thought of Abdul Qadir Audah, who explains that *al-mas'uliyyah al-jinā'iyyah* is a person's capacity to bear legal consequences for a prohibited act if it is committed based on free will and accompanied by knowledge and awareness of the resulting consequences. Based on this view, criminal liability in Islam is founded on at least three main elements, namely: (1) *al-fi'l al-muḥarram* (the existence of a prohibited act), (2) *ikhtiyār* (the exercise of free will in committing the

[24] Syifa Nurul Sabila and Wira Atman, "Studi Kasus Kebocoran Data SIM Card Oleh Bjorka: Dampaknya Terhadap Kepercayaan Publik Terhadap Keamanan Digital Di Indonesia," *Sosial Simbiosis : Jurnal Integrasi Ilmu Sosial Dan Politik* 2, no. 3 (2025): 142–154, https://doi.org/10.62383/sosial.v2i3.1998.

[25] Putri, "Upaya Hukum Dalam Strategi Perlindungan Data Pada Penggunaan Internet Studi Kasus : Hacker Bjorka."

[26] Muhammad Ahmad Farhan and Sadiyah El Adawiyah, "Pengaruh Manajemen Krisis Kasus Hacker Bjorka Terhadap Reputasi Kementerian Komunikasi Dan Informatika," *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 10 (2025): 1993–1999, https://doi.org/10.59141/cerdika.v5i10.2722.

[27] Farhan and Adawiyah.

[28] Aḥmad Fatḥī Al–Bahnasī, *Al-Mas'uliyyah Al-Jinā'iyyah Fī Al-Fiqh Al-Islāmī: Dirāsah Fiqhiyyah Muqāranah* (al–Qahirah: Dar al–Shawq, 1988), h. 27–36.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

act), and (3) *idrāk* (the existence of knowledge and awareness of the consequences arising from the act).[29]

The conceptualisation of *al-mas'uliyyah al-jinā'iyyah* in relation to cybercrime requires more operational parameters so that it does not remain merely at a normative and abstract level. The element of a prohibited act (*al-fi'l al-muḥarram*) can be identified through forms of digital infringement, such as illegal access to electronic systems, data theft, manipulation of electronic information, or the unauthorised dissemination of data, which are legally relevant to Articles 30 and 32 of the ITE Law, as well as Article 65 of the Personal Data Protection Law (PDP Law).[30] The element of free will (*ikhtiyār*) can be assessed through the presence of intent (intentionality), the level of autonomy the perpetrator exercises in utilising technology, and the presence or absence of coercion in carrying out the act. Meanwhile, the elements of knowledge and awareness (*idrāk*) are analysed through the perpetrator's level of understanding of the risks, impacts, and legal consequences of their actions towards the victim, electronic systems, or the public interest. In this context, the dissemination of personal data or unauthorised access to electronic systems as regulated under Article 46 of the ITE Act and Article 67 of the PDP Act indicates that positive law places the emphasis of criminal liability on the proof of the elements of fault and legal consequences, whereas *fiqh jināyah* extends the analysis to include motive, the degree of harm (*darar*), and the threat to the *maṣlaḥah 'āmmah*. Thus, the operationalisation of parameters such as the elements of act, intent and awareness enables the concept of *al-mas'uliyyah al-jinā'iyyah* to be applied more concretely in assessing the criminal liability of cybercriminals. This approach demonstrates that the concept of Islamic criminal liability does not remain confined to the normative—theological level, but can be contextualised in a manner more relevant to the development of modern cybercrime through more measurable indicators, thereby reducing the potential for overly abstract and varied interpretations.

When viewed through the lens of the principle of *al-mas'uliyyah al-jinā'iyyah*, this criminal case clearly fulfils the elements of criminal liability as explained by Abdul Qadir Audah, namely the existence of a prohibited act, the intention to commit it, and awareness of the consequences of the crime committed. The prohibited act in this context includes hacking into the state's security systems, disseminating and trading stolen data; thus, Bjorka's actions have been proven to have disrupted public security, undermined national stability, and violated the *maqāṣhid al-syarī'ah*. Furthermore, the series of digital activities carried out by Bjorka demonstrate the presence of free will, as each act of hacking involved a planning process and an awareness of the implications of his actions; thus, it cannot be described as a spontaneous impulse beyond his control. The statements made by Bjorka across various social media platforms ranging from admissions of his crimes to political propaganda that increasingly shapes public perception further reinforce the argument that the perpetrator understood the impact and purpose of his actions. Consequently, the attacks carried out by Bjorka demonstrate the presence of the element of *'ilm wa idrāk al-natījah* (conscious understanding of the consequences of his actions).

[29] 'Abdul al—Qadir 'Audah, *Al-Tashrī' Al-Jinā'ī Al-Islāmī: Muqāranan Bi Al-Qānūn Al-Waḍ'ī Juz I* (Bayrūt: Mu'assasat al—Risalah, 2013), p.414.

[30] The Government of Indonesia, "Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions" (2024); The Government of Indonesia, "Law No. 27 of 2022 on the Protection of Personal Data" (2022).

This verse forms the legal basis that no one may be punished for a crime they did not commit. However, criminal liability may also be collective; the scholars have developed this through the theory of *al-isytirak fi al-jarīmah* that is, participation in a crime so that any party involved in the planning and execution may be held criminally liable.[31] The majority of jurists distinguish between two main forms of participation in a crime: first, *isytirāk al-mubāsyir* (the perpetrator who participates directly), whether through *tawāfuq* (coincidence) or through *tamālu* (agreement); and secondly, *isytirāk ghayr al-mubāsyir* (indirect participation), comprising those who order, incite, enter into an agreement, or provide technical assistance that enables the commission of the crime.[32] In the context of Bjorka, anyone who carries out hacking or contributes to the commission of a crime is essentially classified as an *isytirāk al-mubāsyir* perpetrator, whilst those who assist or provide security loopholes are classified as *isytirāk ghayr al-mubāsyir* perpetrators, who are held accountable for the entire chain of collective crimes they have committed.

Bjorka's crimes cannot be adequately assessed solely through the technical parameters of positive law; rather, they must be situated within a broader normative framework, namely the Sharia orientation that necessitates the protection of the order and sustainability of human life. The principle of criminal liability from the perspective of *fiqh jināyah* is fundamentally rooted in the *maqāṣhid al-syarī'ah*. Al—Ghazali formulated the objectives of Islamic Sharia as essential pillars, known as the five fundamental principles (*al-ḍarūriyyāt al-khams*), namely the preservation of religion, life, intellect, lineage, and property.[33] On the other hand, Tajuddīn al—Subkī replaced *ḥifẓ al-nasl* (preserving lineage) with *ḥifẓ al-'irḍ* as the preservation of honour.[34] This fundamental principle must be upheld throughout the ages; when any of these pillars is disrupted, social balance and security are likewise shaken.[35]

Fiqh jināyah offers a framework for criminal punishment that is relevant to understanding the complexities of contemporary cybercrime, particularly through several fundamental principles: (1) rehabilitation, which treats punishment as a means of reform and the protection of society; (2) prevention, namely efforts to prevent crime through moral education and the strengthening of social awareness; (3) the consideration of *ḍarar—mafsadah*, by calibrating punishment according to the level of danger and harm; (4) moral transcendence, which affirms that justice derives from divine values; and (5) forgiveness and repentance, which positions sanctions as a means of fostering legal awareness and as a last resort (*ultimum remedium*) after corrective measures have been

[31] 'Audah, *Al-Tashrī' Al-Jinā'ī Al-Islāmī: Muqāranan Bi Al-Qānūn Al-Waḍ'ī Juz I.*

[32] Muhammad Ilham and Suherman Nasution, "Participation In Crimal Acts According In Islamic Criminal Law," *Al-Qanun* 3, no. 2 (2022): 95—105, https://doi.org/10.58836/al—qanun.v3i2.19692.

[33] Dasmadia et al., "Maqasid Al—Shariah and Organizational Performance: A Systematic Literature Review," *Global Review of Islamic Economics and Business* 12, no. 1 (2024): 106—19, https://doi.org/10.14421/grieb.2024.122—03.

[34] Khairul Hamim and Lalu Supriadi bin Mujib, 'The Contextualization of Ḥifẓ Al—'Irḍ on Hoax News (A Study On Imam Tajuddīn Al—Subkī's Maqasid Al—Sharī'a)', *Ulumuna* 24, no. 2 (2020): 348—66, https://doi.org/10.20414/ujis.v24i2.405.

[35] Dhika Tabrozi, "Ijtihad Maqashid Sharia in the Thought of Asy—Syatibi and Muhammad At—Tahir Ibn Ashur," *Al-Mazahib* 13, no. 1 (2025): 1—28, https://doi.org/10.14421/al—mazaahib.v13i1.4068.

exhausted.[36] Within this framework, Islamic criminal law presents a more comprehensive and integrative approach, as it assesses not only violations of individual rights and the social system of society, but also harm to moral values, social security, and public order as part of the protection of the *maqāṣhid al-syarīʻah*.

The Concept of Penalties for Bjorka's Cybercrimes under Islamic Criminal Law

The system of sanctions in Islamic criminal law is known as *ʿuqūbāh*, namely punishments established to protect the public interest in response to violations of Sharia provisions, which serve to uphold social order and act as instruments of education, prevention and moral reform, with a view to creating a just social order through a balance between the public interest and individual rights.[37] The criminal act committed by Bjorka can be classified as a *jarīmah taʻzīr* because there is a prohibition in the naṣh, even though it is not explicitly stated; consequently, the imposition of sanctions is left to the *ulil amri* (leader) or *qadhi* (judge) based on the level of danger and harm caused. *Taʻzīr* is distinguished between the rights of Allah and individual rights, as explained by Mahmud Syaltut: the rights of Allah encompass all matters whose benefits serve the public interest and social welfare, whilst individual rights pertain to the rights of human beings.[38] Consequently, a violation of Allah's rights cannot be nullified once proven, unless the perpetrator ceases the transgression and demonstrates genuine remorse, whereas a violation of human rights can be resolved through reconciliation.[39] When applied to Bjorka's crime, this act not only violates individual rights but has also encroached upon Allah's rights, as the disruption caused has had an impact on the wider community.

In the digital context, the dissemination of false information has become a form of mass deception that undermines *ḥifẓ al-ʿaql* (the preservation of reason). Sumardi Efendi's findings demonstrate that Islamic criminal law views falsehood in cybercrime as a threat that can cause harm, create unrest and undermine social order, as it encompasses various other heinous acts such as slander, false accusations, and even sowing discord, which undermines the principle of honesty; indeed, criminal liability extends not only to the liar but also to those who disseminate such falsehoods.[40] When the public is fed false news and continually steered towards erroneous perceptions, clear thinking weakens, public credibility collapses, and social slander flourishes. The impact is not limited to a single institution, but also extends to the weakening of the collective ability to assess the truth in a sound manner, even though the preservation of reason is one of the main foundations of the *maqāṣhid*.

---

[36] Danial, "Criminalization in Islamic Penal Code: A Study of Principles, Criminalization Methods, and Declining Variations," *Jurnal Ilmiah Peuradeun* 11, no. 3 (2023): 1005–26, https://doi.org/10.26811/peuradeun.v11i3.1058.

[37] Aḥmad Al-Ḥuṣarī, *Al-Siyāsah Al-Jazāʾiyyah: Al-Ḥudūd Wa Al-Ashribah Fī Al-Fiqh Al-Islāmī Juz III* (Bayrūt: Dar al-Jīl, 1993), p.254–256.

[38] Munadi Usman and Abdullah. Kafrawi, "Fuqaha' Perspective on Government Authority in Formulating Ta'zīr Penalty," *Siyasah Wa Qanuniyah : Jurnal Ilmiah Ma'had Aly Raudhatul Ma'arif* 3, no. 1 (2025): 42–57, https://doi.org/10.61842/swq/v3i1.42.

[39] Mukhtor Akramov, "Ta'dhir in Islamic Law : Types of Crimes and Punishments," *Jurnal ISO: Jurnal Ilmu Sosial, Politik Dan Humaniora* 4, no. 2 (2024): 1–7, https://doi.org/10.53697/iso.v4i2.1861.

[40] Sumardi Efendi, "A Comparative of Sanctionsfor Hoax as an Information Crimeunder the Electronic Information and Transactions Law (UU ITE) and Fiqh Jinayah," *Jurnal El-Hadhanah: Indonesian Journal Of Family Law And Islamic Law* 5, no. 1 (2025): 32–45, https://doi.org/10.22373/hadhanah.v5i1.7698.

Bjorka's cyber activities, viewed within the framework of *maqāṣhid*, clearly undermine *ḥifẓ al-māl* by threatening the public's sense of security regarding data ownership. Fageh and Solikhawati firmly argue that digital assets or data, although in the form of data, can essentially be categorised as the concept of wealth in the naṣh or referred to as mamluk assets (assets owned by individuals or legal entities) because they are of benefit to society and can even generate other assets.[41] In line with this, Khairul Azhar Meerangani and others classify digital assets as valuable property and security systems as the modern equivalent of *al-hirz*. This study also emphasises that cybercrime may be categorised as a hudud offence, such as the hadd for theft (*sariqah*); however, due to the need for strict evidentiary standards and the principle of prudence, the hudud penalty is waived due to doubt (*syubhat*).[42] Therefore, any prohibition against various forms of unlawful acquisition of wealth whether through fraud, manipulation, or seizure, carried out covertly or openly is clearly forbidden. One of the fundamental concepts of unlawful appropriation of property in criminal fiqh is known as the hadd for theft (*sariqah*); however, the hacking carried out by Bjorka cannot be classified as *sariqah* because its essential elements are not fulfilled for instance, there is no transfer of tangible property, as digital data and access cannot be physically taken; digital systems cannot be equated with hirz in the classical sense; and the value of information cannot be calculated using the nisab applied under Islamic law.

In the modern context, the concept of *tajassus* is no longer limited to manual surveillance, but has expanded to include systematic hacking, the theft of credentials, and the disclosure of public secrets through technology; yet Islam places great emphasis on human dignity through the principle of *ḥifẓ al-'irḍ* (preserving honour), which affirms that data privacy is a fundamental aspect of human dignity that must be protected.[43] The Qur'an even forbids entering someone's home without permission, as stated in Surah an-Nur, verse 27.

The complexity of such offences increases significantly when they involve strategic government data, as the act of accessing, copying or disseminating sensitive state information used for political pressure, social destabilisation, or even the undermining of state institutions goes beyond mere espionage and falls within the category of digital espionage. At this point, a similarity in pattern emerges with one of the elements of *ḥirābah*, namely the disruption of security, as stated by Abdul Qadir Audah that one of the fundamental elements in the categorisation of the crime of *ḥirābah* is, in essence, instilling fear in others.[44] Security is a fundamental need within the *maqāṣid*; if social security is disrupted, the stability of human life is also threatened.[45] However, objectively speaking, although hacking can cause public anxiety and erode a sense of security, the

[41] Fageh and Solikhawati, "The Bjorka Hacking Phenomenon on Selling Personal Data as a Digital Asset from The Perspective of Maqashid Sharia."

[42] Khairul Azhar Meerangani et al., "Cybercrime and Its Violation of Digital Platform Security: An Islamic Law Perspective," *International Journal of Academic Research in Progressive Education and Development* 11, no. 3 (2022): 503–15, https://doi.org/10.6007/IJARPED/v11-i3/14564.

[43] Munifah and Mufrod Teguh Mulyo, "Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence," *Ulul Albab: Jurnal Studi Dan Penelitian Hukum Islam* 8, no. 2 (2025): 2597–6168, https://doi.org/10.30659/jua.v8i2.44585.

[44] 'Abdul al-Qadir 'Audah, *Al-Tashrī' Al-Jinā'ī Al-Islāmī: Muqāranan Bi Al-Qānūn Al-Waḍ'ī Juz II* (Bayrūt: Mu'assasat al-Risalah, 2013), p.585–587.

[45] Omar bin Ali Muhammad Al-Salami, "The Impact of Objectives Sharia on Achieving and Enhancing Societal Security. Contemporary Readings in Law and Social Justice," *Contemporary Readings in Law and Social Justice* 16, no. 1 (2024): 183–91.

nature of the threat remains indirect. The fear arising from digital disruption differs substantially from the concrete fear characteristic of classical *ḥirābah*, such as physical threats, street attacks, or highway robbery, which place the victim in real danger as is the essence of the crime of *ḥirābah*.

The determination of *ta'zīr* sanctions for Bjorka's criminal acts cannot be standardised, but must be based on the nature of the offence committed. In this study, Bjorka's actions are analysed through the elements of *al-kazb*, *akh al-māl bi ghairi ḥaqq*, and *tajassus*, which are used as parameters in the design of a proportionate *'uqūbah* based on the degree of fault, motive, and social impact. To avoid subjectivity in sentencing, more measurable parameters are required through indicators such as the degree of intent, the extent of social impact, profit orientation, the number of victims, and the threat to the public interest. This approach is consistent with the principle of *al-jazā' min jins al-'amal* (retribution commensurate with the nature of the act),[46] whereby the form of punishment is linked to the nature of the act, so that sanctions are classified into three tiers: light, moderate, and severe, as follows:

Light Ta'zīr may be applied to digital offences involving a low degree of culpability, without any economic motive or intent to harm the public interest, such as the dissemination of invalid information due to negligence, ignorance, or low digital literacy. This category is identified by indicators such as limited social impact, the absence of a profit motive, and a minimal number of victims. In such circumstances, sanctions may be implemented through stern warnings, digital ethics training, proportionate fines, specific access restrictions, or short-term imprisonment. This framework reflects the *ta'dīb* orientation in *fiqh jināyah*, which positions sanctions as both educational and corrective instruments to prevent the recurrence of offences.[47] This is based on the foundation and primary objective of *ta'zīr*, namely *ta'dīb*, as articulated by al-Mawardi, who stated that *ta'zīr* is a sanction in the form of education regarding sinful acts for which no specific sanction has been prescribed by the Sharia.[48] The forms of *ta'dīb* in the imposition of sanctions within the literature of *fiqh jināyah* are highly diverse, as exemplified by the practice of Umar bin al-Khattab when he imposed sanctions for false testimony, including forty lashes, branding the face, shaving the head, parading the offender through the streets, and even extending the duration of imprisonment.[49] This range of penalties is not merely a response to the offence, but also serves as a lesson to the offender to prevent them from reoffending, and as an educational deterrent to the public to prevent similar offences.

Moderate Ta'zīr is applied to acts involving an element of intent, specific motives, and broader implications for privacy and social order, including the misuse of personal data, the manipulation of information, and the distribution of data that causes public

[46] Sultan Sabil Alanazi, Abdul Karim Ali, and Shahidra Abdul Khalil, "Fiqh Adaptation (Al-Takyif Al-Fiqhi) of the Crime of Extortion through Electronic Means and Its Penalties in Islamic Law," *Jurnal Fiqh* 20, no. 1 (2023): 141–64, https://doi.org/10.22452/fiqh.vol20no1.6.

[47] Muhammad Mawardi Djalaluddin et al., "The Implementation of Ta'zīr Punishment as an Educational Reinforcement in Islamic Law," *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (March 31, 2023): 399, https://doi.org/10.22373/sjhk.v7i1.15101.

[48] Vichi Novalia et al., "Ta'zir Dalam Pidana Islam: Aspek Non Material," *Terang : Jurnal Kajian Ilmu Sosial, Politik Dan Hukum* 1, no. 2 (2024): 225–234, https://doi.org/10.62383/terang.v1i2.222.

[49] ʿAbdullah Muḥammad ibn Abī Shaybah, *Al-Muṣannaf Juz XV* (Riyaḍ: Dar Kunūz Ishbīliyyah li al-Nashr wa al-Tawzīʿ, 2015), p.477.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

unrest. In the context of the Bjorka case, the dissemination of personal data and claims of strategic information leaks may be categorised at this level provided they meet the element of intent and are proven to cause significant social harm. Classification indicators include the presence of motive, the extent of the victim base, and the level of disruption to social stability. Sanctions in this category may take the form of flogging (*jald*) within the limits of *ta'zīr* determined by the degree of fault, imprisonment, fines proportionate to the level of harm, exile (*nafy*), or restrictions on digital activities as a form of mitigation against the potential for repeat offences. The imposition of these sanctions is grounded in the principle that *ta'zīr* serves not only as an instrument of retribution but also as an educational tool (*ta'dīb*) and a means of social protection (*ḥimāyah al-mujtama'*) against the systemic impact of an offence. This rationale is grounded in the philosophical basis of Caliph Umar ibn al—Khattab's policy of imposing severe punishments for forgery, such as that committed by Ma'n ibn Za'idah, who lied and abused a position of trust; he was sentenced to flogging accompanied by imprisonment, and then, upon the completion of his imprisonment, Umar imposed two further punishments, each consisting of one hundred lashes, before exiling him.[50] Umar's firm action demonstrates that the manipulation of information and the leaking of public data should be regarded as a form of intellectual betrayal that undermines social trust and the stability of government.

Severe Ta'zīr is applied to cybercrimes that have a systemic impact on national security, governmental stability and public order, such as digital espionage, attacks on strategic infrastructure, or the dissemination of information that causes public panic. Indicators for this category include the level of damage (*darar*), threats to state institutions, and the potential for social disruption. From the perspective of *fiqh jināyah*, this category relates to the protection of the public interest (*ḥifẓ al-niẓām al-'ām*) and is relevant to both cyber terrorism and state espionage. Consequently, severe *ta'zīr* sanctions may include long—term imprisonment, fines proportionate to public losses, flogging (*jald*), exile (*nafy*), permanent restrictions on digital access, and, according to some scholars, the ultimate *ta'zīr* if proven to cause *fasād fī al-arḍ* or threaten national security. The relevance of this category is evident in the Bjorka case, which is linked to the dissemination of personal data and the alleged leak of strategic government information, as such actions not only violate individual privacy but also have the potential to undermine public trust and disrupt national stability. Thus, the orientation of criminalisation is not merely repressive but also preventive, aimed at preventing the recurrence of cybercrimes with systemic impacts. Some scholars do indeed permit the death penalty for spies working on behalf of the enemy, whilst others reject the death penalty, arguing that imprisonment and flogging until the offender repents are sufficient, on the grounds that the Prophet did not impose such a punishment in the case of Hatib bin Abi Balta'ah.[51] However, regardless of these differing opinions, the level of harm remains the benchmark, as in the case of the Bjorka hack, which has the potential to disrupt national security, cause public unrest, and weaken state institutions actions that may be viewed as fasad fī al—arḍ (corruption on earth). Consequently, the penalties may reach the highest level, ranging from exile, the amputation of hands and feet in a crosswise

[50] Aḥmad ibn Ibrahīm Al—Jubayyib, *'Uqūbat Al-Jald Fī Al-Sharī'ah Al-Islāmiyyah* (Makkah: Jami'ah Umm al—Qura, 1986), p.419.

[51] Umaid 'Uthman Al—Kurdī, *'Uqūbat Al-I'dām Fī Al-Syarī'ah Al-Islāmiyyah* (Bayrūt: Mu'assasat al—Risalah, 2008), p.329—331.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

manner, crucifixion, or the death penalty, as legitimised by the Qur'an, Surah al−Ma'idah, verse 33.

The phenomenon of digital offences committed by anonymous cyber actors such as Bjorka represents a form of modern crime that intersects with the fundamental principles of Sharia. The cybercrimes committed by Bjorka reflect a new form of *fasad fī al-arḍ* in the digital context, wherein the elements of *kadzib*, *akhdh al-māl bi ghayr ḥaqq*, and *tajassus* in a digital context all of which pose a threat to the *maqāṣhid al-syarīʿah*, particularly the concepts of *ḥifẓ al-māl*, *ḥifẓ al-ʿirḍ*, and *ḥifẓ al-ʿaql* simultaneously. Although, within the context of *fiqh al-jināyah*, it cannot be equated entirely with the crimes of theft or highway robbery due to the presence of elements of ambiguity in the modus operandi of the criminal act. It is here that Islamic criminal law demonstrates its flexibility and moral depth, as *taʿzīr* is not merely an instrument of punishment, but rather an Islamic criminal policy that combines educational, preventive, and repressive functions to maintain social stability and the moral integrity of the digital society. Through an approach based on *maqāṣhid al-syarīʿah*, criminal jurisprudence is not only capable of adapting to the dynamics of modern technology, but also offers a future legal paradigm that balances justice and security, technology and ethics, as well as power and the public interest.

By comparison, the imposition of penalties for cybercrime under Indonesian positive law is based on the proof of formal legal elements, the degree of fault, and the legal consequences incurred, as stipulated in Law No. 11 of 2008 on Electronic Information and Transactions (EIT Law) and its amendments, and Law No. 27 of 2022 on Personal Data Protection (PDP Law). For example, unauthorised access to an electronic system as provided for in Article 30 of the EIT Law may be subject to criminal sanctions under Article 46, in the form of imprisonment for a maximum of 6−8 years and/or a fine of up to IDR 600−800 million, depending on the severity of the offence.[52] Meanwhile, the unlawful misuse or disclosure of personal data under Article 67 in conjunction with Article 65 of the PDP Act may be punishable by imprisonment of up to 5−6 years and/or a maximum fine of Rp5−6 billion.[53] This approach to criminalisation focuses on the aspects of legality, the proof of criminal elements, and the resulting harm. Conversely, Islamic criminal law (*fiqh jināyah*) considers not only normative violations but also the degree of harm (*darar*) and its impact on the *maqāṣid al-syarīʿah*. As cybercrime is not explicitly regulated in the text of the law, criminal offences such as the Bjorka case are more appropriately classified as *jarīmah taʿzīr*, with penalties determined on the basis of the degree of culpability and the social impact caused, ranging from a stern warning, digital ethics training, a fine (*gharāmah*), flogging (*jald*), imprisonment (*ḥabs*), exile (*nafy*), permanent restriction of access to specific digital systems, and ultimately *taʿzīr* in extreme circumstances that threaten public security or national stability. This comparison demonstrates that positive law places greater emphasis on legal certainty and proportionality of punishment, whereas *fiqh jināyah* broadens the orientation of punishment as an educational, preventive, and repressive instrument aimed at safeguarding the public interest and social stability.

[52] The Government of Indonesia, Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.
[53] The Government of Indonesia, Law No. 27 of 2022 on the Protection of Personal Data.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

DISCUSSION

The phenomenon of cybercrime represents a transformation in modern crime that has evolved alongside technological advances and global connectivity via the internet. The United Nations Office on Drugs and Crime (UNODC) classifies cybercrime as offences that directly target electronic systems, such as hacking and denial—of—service (DoS) attacks, as well as technology—based offences, including identity theft and the distribution of illegal content.[54] This complexity highlights the gap between law in books and law in action, as articulated by Roscoe Pound, namely the situation where technological developments outpace the law's ability to respond to new forms of crime. Consequently, although modern law remains oriented towards the protection of the public interest through the principle of *salus populi suprema lex esto*, regulatory instruments often face limitations in addressing the cross—border nature and dynamics of cybercrime.[55] This situation indicates that the primary challenge in addressing cybercrime lies not only in regulatory limitations, but also in a criminal liability paradigm that has not yet fully adapted to the nature of contemporary digital crime.

The Bjorka case highlights a shift in modern cybercrime, which is no longer limited to unauthorised access to electronic systems, but also encompasses the distribution of personal data, alleged leaks of strategic information, and the potential undermining of public trust in state institutions. From the perspective of Indonesian positive law, such actions may be classified as a violation of Article 30 in conjunction with Article 46 of Law No. 11 of 2008, as amended by Law No. 19 of 2016 on Electronic Information and Transactions, concerning unauthorised access to electronic systems, as well as Article 65 in conjunction with Article 67 of Law No. 27 of 2022 on Personal Data Protection regarding the unlawful acquisition and dissemination of personal data. However, the construction of criminal liability in these regulations tends to rely on the proof of legal—formal elements, fault, and legal consequences, so that the assessment of cybercrime places greater emphasis on the normative—positivist dimension rather than its impact on the wider public interest.

In contrast to this approach, Abdul Qadir Audah's theory of *al-mas'uliyyah al-jinā'iyyah* expands the concept of criminal liability through the elements of a prohibited act, conscious intent, and the capacity to be held responsible. The findings of this study were obtained through a conceptual analysis of the theory of *al-mas'uliyyah al-jinā'iyyah*, which was compared with the elements of cybercrime in Indonesian positive law, the characteristics of Bjorka's actions, and the principles of *fiqh jināyah*. Based on this analysis, Bjorka's actions fulfil the elements of Islamic criminal liability, namely the existence of a prohibited act (*al-fi'l al-muḥarram*), conscious intent (*ikhtiyār*), and awareness of the resulting consequences, and can therefore be classified as a *jarīmah ta'zīr*, as the characteristics of cybercrime are not explicitly regulated in the *naṣh*. This finding demonstrates that the elements of *al-mas'uliyyah al-jinā'iyyah* retain their applicability to cybercrime, even though the object and modus operandi differ from those of classical *jarīmah*. Furthermore, Islamic criminal liability does not stop at the

[54] Muhammad Akram Rana, 'Cybercrime and Digital Fraud Froman Islamic Legal Standpoint', *Journal Of Arts And Social Sciences* 1, no. 1 (2024): 10—22, https://alirfanofficial.com/index.php/hijass/article/view/4.

[55] Orien Effendi and Ro'is Alfauzi, "Dynamics Of Application Of Salus Populi Suprema Lex Esto In Law Enforcement In Indonesia," *Untang Law Review* 5, no. 2 (2021): 40—41, https://doi.org/10.36356/ulrev.v5i2.2633.

Al-Hurriyah : Jurnal Hukum Islam
Vol. 11. No. 1. Edition June 2026

identification of formal offences, but also considers the degree of harm (*darar*), the perpetrator's intent, and the threat to the *maṣlaḥah ʻāmmah*, as reinforced through Al—Shaṭibi's theory of *maqāṣid al-syarīʻah*. Thus, the findings of this study indicate that the limitations of positive law in addressing cybercrime lie not only in regulation, but also in a sentencing paradigm that continues to rely on formal legality without comprehensively integrating the protection of the public interest.

By comparison, Indonesian positive law and *fiqh jināyah* demonstrate differing approaches to establishing criminal liability. Positive law tends to emphasise the proof of legal—formal elements and legal consequences, whereas *fiqh jināyah* broadens this approach through the protection of *maqāṣid al-syarīʻah* and the public interest.[56] This difference indicates that the concept of *taʻzīr* possesses a higher adaptive capacity in responding to contemporary cybercrime, as it allows for the classification of sanctions based on the level of harm, motive, scope of victims, and threats to social stability and public security. Based on these parameters, this study constructs a classification of *taʻzīr* for cybercrime into light, moderate, and severe categories according to the level of harm (*darar*) caused, based on the principle of *al-jazāʼ min jins al-ʻamal*. Thus, Bjorka's actions involving the distribution of personal data, the potential disruption of information security, and the impact on public trust can be classified under a specific level of *taʻzīr* based on the level of threat and the resulting social impact. This finding demonstrates that *taʻzīr* has the potential to be constructed as a more contextual and responsive model of punishment to the characteristics of modern digital crime, without disregarding the principles of proportionality and legal certainty.

The dialogue between criminal jurisprudence (*fiqh jināyah*) and contemporary law enforcement practices is evident in the efforts of several Muslim countries to integrate Sharia principles into cybercrime regulations. Pakistan, through the Prevention of Electronic Crimes Act (PECA) of 2016, demonstrates a form of harmonization between public safety protection and Sharia values, [57] although its implementation still faces challenges regarding the flexibility of legal norms, the potential for multiple interpretations, and the protection of individual rights.[58] This experience demonstrates that the integration of *jināyah* principles into cybercrime regulations is not a utopian construct, but requires a balance between legal flexibility, regulatory certainty, and the protection of human rights. Therefore, the relevance of *taʻzīr* to modern cybercrime lies in its ability to adapt to social change, provided that its implementation continues to consider the principle of legality and the need for public protection in contemporary digital society.

The theoretical contribution of this study lies in a conceptual modification of the classification of *taʻzīr*, which in the literature of *fiqh jināyah* is generally understood in normative terms and lacks operational indicators for contemporary digital crimes. This study modifies the classical classification of *taʻzīr* by adding parameters such as the degree

[56] Adhisty Sitaresmi et al., "Legal Frameworks for Cybersecurity and Data Protection in Cloud—Based Notarial Systems in Indonesia: An Intersectional Analysis of Positive Law and Islamic Legal Principles," *Al-ʻAdalah* 22, no. 1 (2025): 29—62, https://doi.org/10.24042/adalah.v22i1.26813.

[57] Sanaullah, Muswar Sikandar Makol, and Muhammad Asim Shahbaz, "Cyber Law and Islamic Jurisprudence: Addressing Digital Crimes in the Shari'ah Framework," *Tanzur* 6, no. 1 (2025): 34—53.

[58] Hazrat Bilal and Muhammad Akbar Khan, . ". Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective," *Al-Idah* 2, no. 1 (2022): 1—18, https://doi.org/10.37556/al—idah.040.02.0802.

of harm (*darar*), the perpetrator's intent (*mens rea*), scope of victims, social harm, and threats to public security as the basis for classifying sanctions against cybercrime, thereby aligning with the orientation of *'uqūbah* as described by Muḥammad Abū Zahrah, wherein the imposition of sanctions is oriented toward safeguarding the public interest and preventing harm to society's fundamental interests.[59] This modification yields an analytical framework that positions the concept of *ta'zīr* not merely as an abstract punitive instrument, but as a more measurable, adaptive, and applicable model of criminal liability in response to the evolution of contemporary digital crimes, in accordance with the principle of *Shāliḥun likulli zamān wa makān* (a law relevant to every time and place). Thus, the novelty of this research lies not only in the application of *fiqh jināyah* to the Bjorka case but also in the effort to reconstruct the parameters of criminal liability and the classification of sanctions, thereby expanding the conceptual framework of *ta'zīr* theory to make it more relevant to the needs of cyber regulation and law enforcement in the digital age.

CONCLUSION

The research findings indicate that cybercrimes such as the Bjorka case cannot be understood merely as violations of electronic systems or personal data, but also as a form of threat to the public interest (*maṣlaḥah 'āmmah*) that impacts the protection of property (*ḥifẓ al-māl*), honor (*ḥifẓ al-'ird*), reason (*ḥifẓ al-'aql*), and social stability. This finding confirms that *fiqh jināyah*, through the concept of *al-mas'uliyyah al-jinā'iyyah*, possesses adaptive capacity in addressing the complexities of modern cybercrime because criminal liability is not determined solely by legal—formal elements but also considers intent, the degree of harm (*darar*), motive, and the impact on the public interest. Thus, this study reinforces the argument that the concept of *jarīmah ta'zīr* can be constructed as a more contextual instrument of punishment for forms of digital crime that are not explicitly regulated in classical legal sources or positive regulations, which often lag behind technological developments.

Theoretically, this study contributes to the development of contemporary *fiqh jināyah* by formulating a classification of light, moderate, and severe *ta'zīr* based on parameters such as the extent of harm, motive, scope of victims, and threats to the public interest and national security. This classification demonstrates that *ta'zīr* serves not only a repressive function but also integrates educational and preventive objectives in maintaining digital social order. Practically, this study recommends the need to develop cyber law policies that do not rely solely on a legal—formal approach as stipulated in the ITE Law and the PDP Law, but also accommodate the principles of protecting the public interest, proportionality of punishment, and prevention of collective risks. Furthermore, the construction of criminal liability based on *fiqh jināyah* can serve as a conceptual framework for regulators and policymakers in formulating a more adaptive, responsive, and balanced model of cyber law enforcement one that prioritizes legal certainty, substantive justice, and public protection in the era of digital transformation.

ACKNOWLEDGMENTS

The author would like to express his deepest gratitude and appreciation to the Research Scholarship Programme of the Badan Amil Zakat Nasional Republik Indonesia (BAZNAS

[59] Zahrah, *Al-Jarīmah Wa Al-'Uqūbah Fī Al-Fiqh Al-Islāmī*.

RI) for the financial support provided, which enabled this research to be carried out and successfully completed. Appreciation is also extended to the various parties who have contributed to the academic process of this research through their support, feedback, and a conducive intellectual environment. The author would particularly like to thank the academic supervisors for their guidance, mentorship, and valuable scientific input throughout the research process, as well as the international co—authors who have contributed through the exchange of perspectives, academic discussions, and the enrichment of scholarly insights in refining this research. Special appreciation is also extended to Adzanah Mariska Salsabila for the productive discussions, constructive exchange of ideas, and meaningful intellectual support in enriching the perspectives and refining the research concepts. All views, analyses, and conclusions presented in this article are the sole responsibility of the author.

DECLARATIONS

AUTHOR CONTRIBUTION STATEMENT

Zaky Anggara, as the first author, conceived and developed the main research idea, formulated the conceptual and methodological framework, carried out data collection and analysis, interpreted the research findings, and led the process of writing and refining the manuscript. Dr Mohammad Sar'an and Dr Enceng Arif Faizal contributed through academic supervision, critical evaluation, and substantive guidance that strengthened both the scientific structure and the depth of the research analysis. Dr Muhammad Akbar Khan contributed by providing an international academic perspective and comparative insights that reinforced the global relevance and international scientific orientation of this manuscript. All authors participated in the final review of the manuscript and approved its publication.

FUNDING STATEMENT

This research received funding support from the BAZNAS Research Scholarship Programme of the Republic of Indonesia, which made a significant contribution to the conduct of the research and the completion of this manuscript. This support enabled the various stages of the research to be carried out optimally. However, the funding body was not involved in the research design, data collection and analysis, interpretation of results, preparation of the manuscript, or the decision to publish this research. The authors are solely responsible for the entire content, findings, and conclusions presented herein.

DATA AVAIBILITITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

DECLARATION OF INTEREST STATEMENT

The authors declare that they have no financial or non—financial conflicts of interest that could influence the findings in this article.

AI USE STATEMENT

The author states that no artificial intelligence (AI) tools were used in the preparation of this manuscript.

ADDITIONAL INFORMATION

Correspondence and enquiries regarding this research material may be addressed to Zaky Anggara via: zakyanggarastudent@gmial.com

ORCID

Zaky Anggara https://orcid.org/0009−0002−7568−5151
Mohamad Sar'an https://orcid.org/0009−0004−1260−4407
Enceng Arif Faizal https://orcid.org/0009−0007−7431−9777
Muhammad Akbar Khan https://orcid.org/0000−0003−4507−1104

REFERENCES

'Audah, 'Abdul al−Qadir. *Al-Tashri' al-Jina'i al-Islami: Muqaranan bi al-Qanun al-Wad'i*. Juz I. Bayrut: Mu'assasat al−Risalah, 2013.

'Audah, 'Abdul al−Qadir. *Al-Tashri' al-Jina'i al-Islami: Muqaranan bi al-Qanun al-Wad'i*. Juz II. Bayrut: Mu'assasat al−Risalah, 2013.

Aji, Pandam Bayu Seto, and Zain Arfin Utama. "Hukum Sebagai Kenyataan: Teori Sebagai Objek Studi dan Bahan Penelitian." *Al-Zayn* 3, no. 2 (2025): 3682−3683. https://doi.org/10.61104/alz.v3i4.1579.

Akramov, Mukhtor. "Ta'dhir in Islamic Law: Types of Crimes and Punishments." *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora* 4, no. 2 (2024): 1−7. https://doi.org/10.53697/iso.v4i2.1861.

Al−Bahnasi, Ahmad Fathi. *Al-Mas'uliyyah al-Jina'iyyah fi al-Fiqh al-Islami: Dirasah Fiqhiyyah Muqaranah*. al−Qahirah: Dar al−Shawq, 1988.

Al−Husari, Ahmad. *Al-Siyasah al-Jaza'iyyah: al-Hudud wa al-Ashribah fi al-Fiqh al-Islami*. Juz III. Bayrut: Dar al−Jil, 1993.

Al−Jubayyib, Ahmad ibn Ibrahim. *'Uqubat al-Jald fi al-Shari'ah al-Islamiyyah*. Makkah: Jami'ah Umm al−Qura, 1986.

Al−Kurdi, Umaid 'Uthman. *'Uqubat al-I'dam fi al-Shari'ah al-Islamiyyah*. Bayrut: Mu'assasat al−Risalah, 2008.

Al−Salami, Omar bin Ali Muhammad. "The Impact of Objectives Sharia on Achieving and Enhancing Societal Security." *Contemporary Readings in Law and Social Justice* 16, no. 1 (2024): 183−191.

Alanazi, Sultan Sabil, Abdul Karim Ali, and Shahidra Abdul Khalil. "Fiqh Adaptation (Al−Takyif al−Fiqhi) of the Crime of Extortion through Electronic Means and Its Penalties in Islamic Law." *Jurnal Fiqh* 20, no. 1 (2023): 141−164. https://doi.org/10.22452/fiqh.vol20no1.6.

Alfazari, Kalil, Mohamad Azrien Mohamed Adnan, and Tengku Sarinja Aini Tengku Kasim. "Cybercrime in Contemporary Society: An Islamic Worldview on Its Framework, Motivations, and Consequences." *Journal of Islamic Educational Research* 11, no. 1 (2025): 46−62. https://doi.org/10.22452/jier.vol11no1.5.

Altaibi, Hajed A. "The Challenges of Execution of Islamic Criminal Law in Developing Muslim Countries: An Analysis Based on Islamic Principles and Existing Legal Systems." *Cogent Social Sciences* 7, no. 1 (2021): 1−13. https://doi.org/10.1080/23311886.2021.1925413.

Anisa, Lina Nur. "Reformasi Hukum Pidana Islam: Telaah Nalar Arab Muhammad Abed Al−Jabiri." *Journal of Islamic Economic and Law (JIEL)* 2, no. 1 (2025): 1−19. https://doi.org/10.59966/jiel.v2i1.1523.

Aprilianti, Astri. "Efektivitas dan Implementasi Undang−Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi." *Begawan Abioso* 15, no. 1 (2024): 41−50. https://doi.org/10.37893/abioso.v15i1.1002.

Azis, Muh. Ilham, Eril, Andi Muh, Taqiyuddin BN, Abdul Salam, and Ahmad Arief. "Maqasid al-Shari'ah Theory by Imam al-Syatibi." *Anayasa: Journal of Legal Studies* 2, no. 1 (2024): 17–34. https://doi.org/10.61397/ays.v2i1.191.

Badan Siber dan Sandi Negara. *Cybersecurity Monitoring Report 2020 dan 2021*. Jakarta: Biro Hukum dan Komunikasi Publik Badan Siber dan Sandi Negara, 2021.

Bilal, Hazrat, and Muhammad Akbar Khan. "Cyber Crime Legislation in Pakistan: A Critical Analysis from Islamic Law Perspective." *Al-Idah* 2, no. 1 (2022): 1–18. https://doi.org/10.37556/al-idah.040.02.0802.

Chen, Shuai, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, and Chundong Gao. "Exploring the Global Geography of Cybercrime and Its Driving Forces." *Humanities and Social Sciences Communications* 10, no. 71 (2023): 1–10. https://doi.org/10.1057/s41599-023-01560-x.

Danial. "Criminalization in Islamic Penal Code: A Study of Principles, Criminalization Methods, and Declining Variations." *Jurnal Ilmiah Peuradeun* 11, no. 3 (2023): 1005–1026. https://doi.org/10.26811/peuradeun.v11i3.1058.

Dasmadia, Syamsul Hadib, Yang Junchu, Nabila Wahyuningtyas, and Ratna Sesotya Wedadjati. "Maqasid al-Shariah and Organizational Performance: A Systematic Literature Review." *Global Review of Islamic Economics and Business* 12, no. 1 (2024): 106–119. https://doi.org/10.14421/grieb.2024.122-03.

Djalaluddin, Muhammad Mawardi, Bulqia Mas'ud, Dedy Sumardi, Isnawardatul Bararah, and Kamus Kamus. "The Implementation of Ta'zir Punishment as an Educational Reinforcement in Islamic Law." *Samarah: Jurnal Hukum Keluarga dan Hukum Islam* 7, no. 1 (2023): 399–425. https://doi.org/10.22373/sjhk.v7i1.15101.

Efendi, Sumardi. "A Comparative of Sanctions for Hoax as an Information Crime under the Electronic Information and Transactions Law (UU ITE) and *Fiqh Jinayah*." *Jurnal El-Hadhanah: Indonesian Journal of Family Law and Islamic Law* 5, no. 1 (2025): 32–45. https://doi.org/10.22373/hadhanah.v5i1.7698.

Effendi, Orien, and Ro'is Alfauzi. "Dynamics of Application of *Salus Populi Suprema Lex Esto* in Law Enforcement in Indonesia." *Untang Law Review* 5, no. 2 (2021): 40–41. https://doi.org/10.36356/ulrev.v5i2.2633.

Fageh, Achmad, and Anisa Solikhawati. "The Bjorka Hacking Phenomenon on Selling Personal Data as a Digital Asset from the Perspective of *Maqashid Sharia*." *Jurnal Hukum Islam* 20, no. 2 (2022): 279–354. https://doi.org/10.28918/jhi.v20i2.6387.

Farhan, Muhammad Ahmad, and Sadiyah El Adawiyah. "Pengaruh Manajemen Krisis Kasus Hacker Bjorka terhadap Reputasi Kementerian Komunikasi dan Informatika." *Cerdika: Jurnal Ilmiah Indonesia* 5, no. 10 (2025): 1993–1999. https://doi.org/10.59141/cerdika.v5i10.2722.

Fitrian, Yuko. "Cyber Terrorism: Analisis Hukum Pidana Mengenai Serangan Bjorka terhadap Data Negara." *Arus Jurnal Sosial dan Humaniora* 3, no. 3 (2023): 164–174. https://doi.org/10.57250/ajsh.v3i3.278.

Habibani, Rhaysya Admmi, Siti Fatimah, and Azmi Fitrisia. "Positivisme: Konsep, Perkembangan, dan Implementasi dalam Kajian Ilmu Pengetahuan dan Hukum." *Cendekia: Jurnal Ilmu Pengetahuan* 4, no. 4 (2024): 524–532. https://doi.org/10.51878/cendekia.v4i4.3831.

Hamim, Khairul, and Lalu Supriadi bin Mujib. "The Contextualization of *Hifz al-'Ird* on Hoax News (A Study on Imam Tajuddin al-Subki's *Maqasid al-Shari'ah*)." *Ulumuna* 24, no. 2 (2020): 348–366. https://doi.org/10.20414/ujis.v24i2.405.

Ilham, Muhammad, and Suherman Nasution. "Participation in Criminal Acts According to Islamic Criminal Law." *Al-Qanun* 3, no. 2 (2022): 95–105. https://doi.org/10.58836/al-qanun.v3i2.19692.

Jacky, M., and F. X. Sri Sadewo. "Indonesian Blogger Analyzing Bjorka Hacker." *Technium Social Sciences Journal* 50, special issue (2023): 532–542. https://doi.org/10.47577/tssj.v50i1.9937.

Juned, Mansur, Ali Martin, and Nugraha Pratama. "Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity." *Academic Journal of Interdisciplinary Studies* 13, no. 5 (2024): 369–380. https://doi.org/10.36941/ajis-2024-0171.

Meerangani, Khairul Azhar, Ahmad Faqih Ibrahim, Muhammad Yasin Omar Mukhtar, Muhammad Asyraf Ahmad Termimi, Muhammad Hilmi Mat Johar, and Adam Badhrulhisham. "Cybercrime and Its Violation of Digital Platform Security: An Islamic Law Perspective." *International Journal of Academic Research in Progressive Education and Development* 11, no. 3 (2022): 503–515. https://doi.org/10.6007/IJARPED/v11-i3/14564.

Muda, Zulkifly, Nizaita Omar, and Nehaluddin Ahmed. "Comparison Between Islamic Criminal Law and Man-Made Law." *International Journal of Academic Research in Business and Social Sciences* 14, no. 2 (2024): 972–980. https://doi.org/10.6007/IJARBSS/v14-i2/20718.

Munifah, and Mufrod Teguh Mulyo. "Personal Data Hacking: A Critical Analysis of Islamic Criminal Law and Islamic Jurisprudence." *Ulul Albab: Jurnal Studi dan Penelitian Hukum Islam* 8, no. 2 (2025). https://doi.org/10.30659/jua.v8i2.44585.

Novalia, Vichi, Laudza Hulwatun Azizah, Novinda Al-Islami, and Surya Sukti. "Ta'zir dalam Pidana Islam: Aspek Nonmaterial." *Terang: Jurnal Kajian Ilmu Sosial, Politik dan Hukum* 1, no. 2 (2024): 225–234. https://doi.org/10.62383/terang.v1i2.222.

Nurulita, Safrida, and Ridwan. "Political Will of the Indonesian Government in Addressing Data Leakage and Cybersecurity in the Era of Digital Transformation." *JHSS (Journal of Humanities and Social Studies)* 9, no. 1 (2025): 28–38. https://doi.org/10.33751/jhss.v9i1.33.

Pastika, I Wayan, Eirenne Pridari Sinsya Dewi, and Ida Bagus Gede Dharma Putra. "Language Cases Against UU ITE in Indonesia." *International Journal of Linguistics, Literature and Culture* 9, no. 5 (2023): 198–208. https://doi.org/10.21744/ijllc.v9n5.2361.

Putri, Annisa Nadya. "Upaya Hukum dalam Strategi Perlindungan Data pada Penggunaan Internet: Studi Kasus Hacker Bjorka." *Jurnal Hukum dan Pembangunan Ekonomi* 12, no. 1 (2024): 52–64. https://doi.org/10.20961/hpe.v12i1.81910.

Putri, Inayah Fasawwa, and Moody Rizqy Syailendra Putra. "Criminal Liability of Perpetrators of SIM Card Registration Data Hacking under the EIT Law and the PDP Law." *Awang Long Law Review* 8, no. 1 (2025): 212–222. https://doi.org/10.56301/awl.v8i1.1909.

Rana, Muhammad Akram. "Cybercrime and Digital Fraud from an Islamic Legal Standpoint." *Journal of Arts and Social Sciences* 1, no. 1 (2024): 10–22.

Sabila, Syifa Nurul, and Wira Atman. "Studi Kasus Kebocoran Data SIM Card oleh Bjorka: Dampaknya terhadap Kepercayaan Publik terhadap Keamanan Digital di Indonesia." *Sosial Simbiosis: Jurnal Integrasi Ilmu Sosial dan Politik* 2, no. 3 (2025): 142–154. https://doi.org/10.62383/sosial.v2i3.1998.

Sanaullah, Muswar Sikandar Makol, and Muhammad Asim Shahbaz. "Cyber Law and Islamic Jurisprudence: Addressing Digital Crimes in the Shari'ah Framework." *Tanzur* 6, no. 1 (2025): 34–53.

Shaybah, 'Abdullah Muhammad ibn Abi. *Al-Musannaf*. Juz XV. Riyad: Dar Kunuz Ishbiliyyah li al–Nashr wa al–Tawzi', 2015.

Sitaresmi, Adhisty, Mas Rahmah, Suparto Wijoyo, and Adhitya Panji Anom. "Legal Frameworks for Cybersecurity and Data Protection in Cloud–Based Notarial Systems in Indonesia: An Intersectional Analysis of Positive Law and Islamic Legal Principles." *Al-'Adalah* 22, no. 1 (2025): 29–62. https://doi.org/10.24042/adalah.v22i1.26813.

Sutikno, Tole, and Deris Stiawan. "Cyberattacks and Data Breaches in Indonesia by Bjorka: Hacker or Data Collector?" *Bulletin of Electrical Engineering and Informatics* 11, no. 6 (2022): 2989–2994. https://doi.org/10.11591/eei.v11i6.4854.

Syah, Radika Hanny, and Muhammad Irwan Padli Nasution. "Analisis Keamanan Siber dan Hukum: Studi Kasus Bjorka." *Jurnal Ilmiah Ekonomi, Manajemen, Bisnis dan Akuntansi* 2, no. 3 (2025): 329–338. https://doi.org/10.61722/jemba.v2i3.948.

Tabrozi, Dhika. "Ijtihad Maqashid Sharia in the Thought of Asy–Syatibi and Muhammad At–Tahir Ibn Ashur." *Al-Mazahib* 13, no. 1 (2025): 1–28. https://doi.org/10.14421/al–mazaahib.v13i1.4068.

The Government of Indonesia. *Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions*. Jakarta: State Secretariat of the Republic of Indonesia, 2024.

The Government of Indonesia. *Law No. 27 of 2022 on the Protection of Personal Data*. Jakarta: State Secretariat of the Republic of Indonesia, 2022.

Usman, Munadi, and Abdullah Kafrawi. "Fuqaha' Perspective on Government Authority in Formulating Ta'zir Penalty." *Siyasah wa Qanuniyah: Jurnal Ilmiah Ma'had Aly Raudhatul Ma'arif* 3, no. 1 (2025): 42–57. https://doi.org/10.61842/swq.v3i1.42.

Wahyuni, Fitri. *Hukum Pidana Islam: Akulturasi Nilai-Nilai Hukum Pidana Islam dalam Pembaharuan Hukum Pidana Indonesia*. Tangerang Selatan: PT Nusantara Persada Utama, 2018.

Zahrah, Muhammad Abu. *Al-Jarimah wa al-'Uqubah fi al-Fiqh al-Islami*. al–Qahirah: Dar al–Fikr al–'Arabi, 1998.