

## **Perbandingan Perspektif Hukum Pencegahan Kejahatan Dunia Maya dalam Hukum Positif dan Hukum Pidana Islam**

Zulfahmi

zulfahmi1901@gmail.com

Putra Aulia

nasutionputra8412@gmail.com

Maulana Muklis

maulanamuklis01@gmail.com

Rosdewi Pulungan

rosdewip@gmail.com

Sekolah Tinggi Agama Islam Negeri Mandailing Natal

### **Abstract**

*The development of information and communication technology in the digital era has changed the way humans interact and access information, while increasing efficiency in various sectors. However, these advancements also pose serious challenges, especially in terms of digital security. This research aims to identify the limitations of Indonesia's positive legal regulations in addressing cybercrime and explore the potential integration of Islamic criminal law principles to improve the effectiveness of law enforcement and prevention. Using a normative legal approach, analysis is conducted on legislation, legal doctrine, and related literature. The results show that cybercrimes such as hacking, phishing and cyberbullying pose significant material, psychological and social impacts on individuals, businesses and national security. While the Electronic Information and Transaction (ITE) Law stipulates penalties of up to 10 years in prison or fines of up to Rp10 billion, law enforcement is often hampered by the difficulty of proving digital evidence, the anonymity of perpetrators, and jurisdictional limitations. From the perspective of Islamic criminal law, cybercrime is categorized as a ta'zir criminal offense, which allows judges to determine punishment according to the level of the offense, while emphasizing restorative justice and deterrence through repentance, as well as moral guidance. This study proposes an integrative strategy between the two legal systems and Islamic ethical principles to more effectively address digital crimes in Indonesia.*

*Keyword: Cyber Crime, Islamic Criminal Law, Positive Law, Ta'zir.*

### **Abstrak**

Perkembangan teknologi informasi dan komunikasi di era digital telah mengubah cara manusia berinteraksi dan mengakses informasi, sekaligus meningkatkan efisiensi di berbagai sektor. Namun, kemajuan ini juga menimbulkan tantangan serius, terutama dalam hal keamanan digital. Penelitian ini bertujuan mengidentifikasi keterbatasan peraturan hukum positif Indonesia dalam menangani kejahatan dunia maya serta mengeksplorasi potensi integrasi prinsip-prinsip hukum pidana Islam guna meningkatkan efektivitas penegakan hukum dan pencegahan. Dengan pendekatan hukum normatif, analisis dilakukan terhadap peraturan perundang-undangan, doktrin hukum, dan literatur terkait. Hasil penelitian menunjukkan bahwa kejahatan dunia maya seperti peretasan, *phishing*, dan *cyberbullying* menimbulkan dampak material, psikologis, dan sosial yang signifikan terhadap individu, bisnis, dan keamanan nasional. Walaupun Undang-undang Informasi dan Transaksi Elektronik (ITE) menetapkan hukuman hingga 10 tahun penjara atau denda mencapai Rp10 miliar, penegakan hukum sering terhambat oleh kesulitan pembuktian bukti digital, anonimitas pelaku, dan keterbatasan yurisdiksi. Dari perspektif hukum pidana Islam, kejahatan dunia maya dikategorikan sebagai tindak pidana *ta'zir*, yang memungkinkan hakim menetapkan hukuman sesuai tingkat pelanggaran, sekaligus menekankan keadilan restoratif dan pencegahan melalui taubat nasuha, serta bimbingan moral. Studi ini mengusulkan strategi integratif antara kedua sistem hukum dan prinsip etika Islam untuk mengatasi kejahatan digital secara lebih efektif di Indonesia.

Kata Kunci: Kejahatan Dunia Maya, Hukum Pidana Islam, Hukum Positif, *Ta'zir*.

#### **A. Pendahuluan**

Kemajuan teknologi informasi dan komunikasi di era digital telah mengubah berbagai aspek kehidupan manusia secara signifikan. Hal ini bukan hanya mempercepat arus informasi dan komunikasi global, tetapi juga membawa berbagai manfaat besar, mulai dari kemudahan akses terhadap informasi, hingga peningkatan efisiensi di sektor ekonomi, pendidikan, pemerintahan, dan hampir setiap aspek kehidupan beralih ke dalam ruang digital.<sup>1</sup> Namun, kemajuan ini juga menghadirkan tantangan baru, terutama yang terkait dengan aspek keamanan. Salah satu tantangan yang muncul adalah

---

<sup>1</sup> Dagm Alemayehu Tegegn, "The Role of Science and Technology in Reconstructing Human Social History: Effect of Technology Change on Society," *Cogent Social Sciences* 10, no. 1 (2024), <https://doi.org/10.1080/23311886.2024.2356916>.

meningkatnya kejahatan yang dilakukan secara digital yang dikenal sebagai *cyber crime* atau kejahatan dunia maya.

*Cyber crime* mencakup berbagai tindakan ilegal yang menggunakan internet atau perangkat digital sebagai sarana utama, mulai dari penipuan daring hingga peretasan.<sup>2</sup> Meningkatnya volume data pribadi dan informasi sensitif yang beredar di dunia maya memberikan peluang bagi pelaku kejahatan untuk mengeksploitasi celah keamanan.<sup>3</sup> Fenomena ini tidak hanya merugikan individu yang menjadi korban, tetapi juga dapat berdampak pada perusahaan, instansi pemerintah, dan keamanan nasional. Kejahatan ini memerlukan regulasi khusus yang mampu mengatur segala bentuk aktivitas kriminal yang terjadi di dunia maya, sebab regulasi di Indonesia saat ini masih terus beradaptasi untuk menjangkau kejahatan ini yang berkembang dengan cepat.<sup>4</sup>

Beberapa penelitian menyoroti bahwa hukum positif yang ada seringkali masih kurang tanggap dalam menghadapi *cyber crime*. Hapsari & Pambayun<sup>5</sup> menyimpulkan bahwa ancaman *cyber crime* di Indonesia sekarang ini tergolong serius karena berpotensi sangat tinggi menimbulkan permasalahan nasional. Pansariadi & Soekorini<sup>6</sup> dalam penelitiannya menyatakan bahwa perlunya merevisi peraturan terkait kejahatan ini untuk mengoptimalkan penegakan hukumnya di Indonesia. Penelitian lain oleh Gunawan<sup>7</sup> mengungkapkan, dalam aturan-aturan di dalam hukum pidana Islam bahwa setiap pelaku *cyber crime* dapat dijatuhi hukuman *ta'zir* bahkan hukuman *hudud* apabila memiliki *'illat* yang sama dengan *jarimah hudud*. Di sisi lain.

Fenomena *cyber crime* ini masih menjadi isu yang relatif baru dalam kajian hukum Islam, karena sebagian besar literatur klasik belum secara

---

<sup>2</sup> Joanna Curtis and Gavin Oxburgh, "Understanding Cybercrime in 'Real World' Policing and Law Enforcement," *The Police Journal: Theory, Practice and Principles* 96, no. 4 (2023): 573–92, <https://doi.org/10.1177/0032258X221107584>.

<sup>3</sup> Gargi Sarkar and Sandeep K. Shukla, "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies," *Journal of Economic Criminology* 2 (2023): 100034, <https://doi.org/10.1016/j.jeconc.2023.100034>.

<sup>4</sup> Awaludin Marwan, Diana Odier-Contreras Garduño, and Fiammetta Bonfigli, "Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia," *BESTUUR* 10, no. 1 (2022): 22, <https://doi.org/10.20961/bestuur.v10i1.59143>.

<sup>5</sup> "Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Konstituen* 5, no. 1 (2023): 1–17, <https://doi.org/10.33701/jk.v5i1.3208>.

<sup>6</sup> "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya," *Binamulia Hukum* 12, no. 2 (2023): 287–98, <https://doi.org/10.37893/jbh.v12i2.605>.

<sup>7</sup> "Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah," *Jurnal El-Qanuniy: Jurnal Ilmu-Ilmu Kesyarahan Dan Pranata Sosial* 6, no. 1 (2020): 96–110, <https://doi.org/10.24952/el-qanuniy.v6i1.2473>.

eksplisit mengatur kejahatan di dunia maya. Akibatnya, banyak pandangan ulama yang berbeda mengenai penerapan hukum Islam dalam konteks ini. Tantangan lainnya adalah pemahaman dan adaptasi hukum Islam terhadap teknologi yang terus berubah dan berkembang pesat. Mengingat hukum Islam didasarkan pada prinsip-prinsip yang sifatnya universal,<sup>8</sup> maka perlu ada pendekatan yang komprehensif untuk mengkaji kesesuaian antara prinsip-prinsip hukum Islam dengan kebutuhan regulasi modern saat ini. Karena setiap jenis kejahatan *cyber crime* memiliki karakteristik yang berbeda dan memerlukan penanganan hukum yang tepat untuk mengatasi dampaknya terhadap korban dan masyarakat.<sup>9</sup>

Penelitian ini berfokus pada beberapa masalah utama yang berkaitan dengan kejahatan dunia maya atau *cyber crime* dengan memberikan definisi yang jelas, ruang lingkup kejahatan, serta menjelaskan jenis-jenis *cyber crime*. Selain itu, penelitian ini juga akan mengkaji bagaimana hukum positif dan hukum pidana Islam, merespons serta mengatur tindakan *cyber crime* dari aspek regulasi hingga implementasi hukumnya. Tujuan utama penelitian ini adalah untuk memberikan pemahaman baru yang komprehensif mengenai kemungkinan penerapan hukum pidana Islam dalam menangani *cyber crime*, serta menyarankan strategi penegakan hukum yang lebih inklusif dan adaptif di era digital.

## **B. Metode Penelitian**

Metode penelitian yang digunakan dalam artikel ini adalah penelitian hukum normatif dengan pendekatan deskriptif. Penelitian ini mengumpulkan data dari sumber primer berupa peraturan perundang-undangan yang mengatur *cyber crime*, seperti Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Kitab Undang-undang Hukum Pidana (KUHP), buku-buku klasik hingga kontemporer mengenai hukum pidana Islam, serta sumber sekunder seperti buku, jurnal, dan literatur terkait. Teknik pengumpulan data dilakukan melalui kajian pustaka sistematis untuk mengidentifikasi doktrin dan regulasi yang relevan,<sup>10</sup> sementara teknik analisis

---

<sup>8</sup> Wael B. Hallaq, *An Introduction to Islamic Law* (Cambridge: Cambridge University Press, 2009).

<sup>9</sup> So-Hyun Lee, Ilwoong Kang, and Hee-Woong Kim, "Understanding Cybercrime from a Criminal's Perspective: Why and How Suspects Commit Cybercrimes?," *Technology in Society* 75 (2023): 102361, <https://doi.org/10.1016/j.techsoc.2023.102361>.

<sup>10</sup> Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, Dan R&D*, Cet. 26 (Bandung: Alfabeta, 2017).

data bersifat deskriptif dengan membandingkan penerapan prinsip-prinsip hukum pidana Islam dan hukum positif dalam menangani kejahatan dunia maya guna mengidentifikasi kesamaan, perbedaan, dan efektivitas regulasi yang ada.<sup>11</sup> Metode ini digunakan untuk menyusun argumentasi yang komprehensif mengenai penanganan *cyber crime* dalam perspektif hukum positif dan hukum pidana Islam.

### C. Pembahasan dan Hasil Penelitian

Definisi yang tepat dan jelas mengenai *cyber crime* atau kejahatan dunia maya dalam konteks akademis masih jarang ditemukan. Istilah ini sering kali disamakan dengan berbagai terminologi lain, seperti “kejahatan elektronik,” “kejahatan komputer,” “kejahatan berbasis komputer,” “kejahatan berteknologi tinggi,” atau “kejahatan yang didorong oleh teknologi.” Dengan kata lain, setiap tindakan kriminal yang memanfaatkan teknologi internet dapat digolongkan sebagai kejahatan dunia maya.<sup>12</sup> Para pelaku kerap memanfaatkan kelemahan yang ada dengan cara-cara tertentu, menjadikan korban sebagai pihak yang terjebak dalam proses viktimisasi. Teknik eksploitasi yang digunakan antara lain termasuk rekayasa sosial, manipulasi keputusan melalui tekanan waktu atau otoritas yang dirasakan, serta pemanfaatan pola kebiasaan yang dapat diprediksi, seperti penggunaan situs web, pengunduhan, kata sandi, dan interaksi di jejaring sosial atau profesional.<sup>13</sup>

Para peneliti membagi kejahatan dunia maya menjadi dua kategori utama, yaitu kejahatan yang bergantung pada dunia maya dan kejahatan yang didorong oleh dunia maya. Kejahatan pertama mencakup pelanggaran yang secara intrinsik terkait dengan teknologi digital, seperti peretasan, dan serangan siber. Kejahatan yang kedua mencakup tindak pidana konvensional yang meskipun telah ada sebelum era internet, kini semakin dipercepat dan

---

<sup>11</sup> John W. Creswell and J. David Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, ed. Helen Salmon et al., 5th ed. (Thousand Oaks, California: Sage Publications, Inc., 2018), <https://lccn.loc.gov/2017044644>.

<sup>12</sup> Curtis and Oxburgh, “Understanding Cybercrime in ‘Real World’ Policing and Law Enforcement.”

<sup>13</sup> Jason R. C. Nurse, “Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit,” in *The Oxford Handbook of Cyberpsychology*, ed. Alison Attrill-Smith et al. (Oxford: Oxford University Press, 2019), 662–90, <https://doi.org/10.1093/oxfordhb/9780198812746.013.35>.

diperburuk oleh kemajuan teknologi digital.<sup>14</sup> Berikut beberapa kategori utama kejahatan dunia maya atau *cyber crime* yang sering terjadi dalam praktik:

**Tabel 1.** Jenis-jenis Kejahatan Dunia Maya

No.	Jenis Kejahatan	Deskripsi
1.	<i>Hacking</i> (peretasan situs web)	Tindakan mengakses sistem komputer atau jaringan tanpa izin yang bertujuan untuk mencuri data, merusak sistem, atau aktivitas ilegal lainnya. <sup>15</sup>
2.	<i>Phishing</i> (penipuan dunia maya)	Penipuan memanfaatkan media seperti email, pesan, atau situs web palsu untuk menipu korban dan memperoleh informasi pribadi, seperti kata sandi, nomor kartu kredit, atau data lainnya. <sup>16</sup>
4.	<i>Cyberstalking</i> (penguntitan dunia maya)	Bentuk pelanggaran di dunia digital di mana pelaku secara berulang kali mengganggu, mengancam, atau memata-matai korban melalui internet.
5.	<i>Cyberbullying</i> (perundungan dunia maya)	Tindakan intimidasi atau pelecehan yang dilakukan melalui platform digital seperti media sosial dan aplikasi pesan instan, seperti penyebaran rumor, ancaman, atau berkomentar kasar. <sup>17</sup>
6.	<i>Online money laundering</i> (pencucian uang daring)	Proses untuk menyembunyikan asal-usul uang yang diperoleh dari kegiatan ilegal melalui transaksi digital. Pelaku memanfaatkan <i>platform</i> keuangan <i>online</i> untuk memindahkan atau “membersihkan” uang tersebut agar tidak terdeteksi sebagai hasil kejahatan. <sup>18</sup>
7.	<i>Identity thieving</i> (pencurian)	Tindakan memperoleh informasi pribadi seseorang secara ilegal dengan tujuan untuk digunakan dalam

<sup>14</sup> You Zhou et al., “Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality,” *Asian Journal of Criminology* 19, no. 3 (2024): 419–39, <https://doi.org/10.1007/s11417-024-09436-y>.

<sup>15</sup> Nurse, “Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.”

<sup>16</sup> Gagandeep Kaur et al., “Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime,” in *Engineering Proceedings* (Basel Switzerland: MDPI, 2024), 6, <https://doi.org/10.3390/engproc2024062006>.

<sup>17</sup> Ahmad Mohamad Alomar and Hassan Sami Alabady, “The Phenomenon of Cyber Bullying: Interpretation, Confrontation, and the Position of Islamic Law,” *Journal of Namibian Studies: History Politics Culture* 34 (2023): 746–768, <https://doi.org/10.59670/jns.v34i.1123>.

<sup>18</sup> Mariem Mejri et al., “Effect of Cultural Tightness-Looseness on Money Laundering: A Cross-Country Study,” *Journal of Money Laundering Control* 25, no. 2 (2022): 414–26, <https://doi.org/10.1108/JMLC-03-2021-0025>.

---

identitas)	transaksi penipuan atau tindakan yang merugikan lain, baik secara finansial maupun reputasional. <sup>19</sup>
------------	--

---

Dari beragam jenis kejahatan dunia maya pada Tabel 1 di atas, kejahatan-kejahatan ini tidak hanya merugikan individu, tetapi juga dapat merusak sistem keamanan dan menyebabkan kerugian materiil maupun immateriil. Dampak dari kejahatan tersebut berpotensi meluas, mengganggu tatanan sosial, dan menimbulkan ketidakpastian yang mengancam kepercayaan masyarakat dalam berinteraksi secara daring. Dampak kejahatan dunia maya terhadap korban sering kali jauh lebih besar dari yang diperkirakan. Kejahatan ini tidak hanya menyebabkan kerugian langsung, tetapi juga berpotensi menimbulkan dampak psikologis yang mendalam, seperti stres dan kecemasan. Di tingkat yang lebih luas, kejahatan dunia maya dapat merusak kepercayaan sosial, terutama dalam konteks interaksi daring, yang dapat mengurangi efektivitas komunikasi digital dan memengaruhi stabilitas sosial secara keseluruhan.<sup>20</sup>

Kejahatan dunia maya atau *cyber crime* di Indonesia diatur oleh sejumlah peraturan perundang-undangan yang relevan. Selain Kitab Undang-Undang Hukum Pidana (KUHP), regulasi utama yang mengatur tindak pidana di dunia maya adalah Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang telah mengalami dua kali perubahan. *Pertama*, melalui UU No. 19 Tahun 2016, dan *kedua*, dengan perubahan terbaru yang tercantum dalam Undang-undang Nomor 1 Tahun 2024. Tidak terdapat pertentangan antara ketentuan yang ada dalam KUHP dan UU ITE terkait pengaturan tindak pidana penipuan yang dilakukan melalui media digital. Kedua peraturan tersebut dapat diterapkan secara bersamaan, dengan ketentuan *Lex Specialis derogat legi Generalis* yang mengutamakan peraturan yang lebih khusus.<sup>21</sup> Berikut ini adalah pasal-pasal yang mengatur berbagai tindak pidana *cyber crime* dalam UU ITE:<sup>22</sup>

### **Tabel 2.** Pasal-pasal yang Mengatur *Cyber Crime* dalam UU ITE

---

<sup>19</sup> Shareen Irshad and Tariq Rahim Soomro, "Identity Theft and Social Media," *IJCSNS International Journal of Computer Science and Network Security* 18, no. 1 (2018): 43-55, [http://paper.ijcsns.org/07\\_book/201801/20180106.pdf](http://paper.ijcsns.org/07_book/201801/20180106.pdf).

<sup>20</sup> Curtis and Oxburgh, "Understanding Cybercrime in 'Real World' Policing and Law Enforcement."

<sup>21</sup> Pansariadi and Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya."

<sup>22</sup> Republik Indonesia, "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952)," 2024.

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

No.	Pasal	Deskripsi
1.	Pasal 27 ayat (1) UU ITE	Mengatur tentang larangan penyebaran informasi yang mengandung muatan kesusilaan, baik melalui siaran, pertunjukan, distribusi, transmisi, atau pemberian akses terhadap informasi elektronik dan dokumen elektronik yang melanggar norma kesusilaan. Pelanggaran terhadap ketentuan ini mengancam pidana penjara paling lama enam tahun dan/atau denda paling banyak satu miliar rupiah.
2.	Pasal 27 ayat (2) UU ITE	Melarang distribusi dan transmisi informasi elektronik atau dokumen elektronik yang mengandung unsur perjudian. Kejahatan ini dapat dijatuhi hukuman pidana penjara hingga sepuluh tahun dan/atau denda maksimal sepuluh miliar rupiah.
3.	Pasal 27 ayat (3) UU ITE	Melarang penyebaran informasi yang mengandung penghinaan dan pencemaran nama baik, yang dilakukan tanpa hak dan sengaja. Jika terbukti melanggar, pelaku dapat dikenai pidana penjara hingga empat tahun dan/atau denda maksimal tujuh ratus lima puluh juta rupiah.
4.	Pasal 27 ayat (4) UU ITE	Mengatur larangan pemerasan dan pengancaman melalui media elektronik. Kejahatan ini dikenakan pidana penjara paling lama enam tahun dan/atau denda hingga satu miliar rupiah.
5.	Pasal 28 ayat (1) UU ITE	Melarang penyebaran berita bohong atau menyesatkan yang dapat merugikan konsumen dalam transaksi elektronik
6.	Pasal 28 ayat (2) UU ITE	Setiap orang yang dengan sengaja dan tanpa hak mentransmisikan atau mendistribusikan informasi yang mengandung unsur kebencian atau permusuhan berdasarkan Suku, Agama, Ras, dan Antargolongan, dapat dikenakan pidana penjara hingga enam tahun dan/atau denda maksimal satu miliar rupiah.
7.	Pasal 29 UU ITE	Mengatur larangan mengirimkan informasi yang berisi ancaman kekerasan atau menakut-nakuti. Pelanggaran terhadap pasal ini dapat dikenai pidana penjara hingga empat tahun dan/atau denda maksimal tujuh ratus lima puluh juta rupiah.
8.	Pasal 30 UU ITE	Mengatur tentang larangan mengakses komputer atau sistem elektronik milik orang lain tanpa izin atau



## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

---

	melawan hukum. Pidana yang dapat dijatuhkan bagi pelanggar pasal ini adalah penjara hingga enam tahun dan/atau denda maksimal enam ratus juta rupiah, dengan peningkatan hukuman bagi pelanggaran yang lebih serius, seperti upaya memperoleh informasi elektronik secara ilegal atau menerobos sistem pengamanan.
10. Pasal 31 ayat (1) UU ITE	Melarang penyadapan informasi elektronik dan dokumen elektronik tanpa izin yang sah. Pelanggaran terhadap ketentuan ini dapat dijatuhi hukuman pidana.
11. Pasal 52 UU ITE	Mengatur tentang penambahan ancaman pidana jika perbuatan yang tercantum dalam Pasal 30 hingga Pasal 37 ditujukan terhadap sistem elektronik yang digunakan oleh pemerintah atau badan strategis, serta dalam kasus tindak pidana oleh korporasi.

---

Dalam hukum pidana Islam, tindak pidana yang tergolong dalam *cyber crime* dapat dikenakan hukuman *ta'zir*.<sup>23</sup> Secara bahasa, *ta'zir* berarti pencegahan (*al-man'u*), sementara dalam terminologi hukum Islam, *ta'zir* merujuk pada hukuman edukatif (*ta'dib*) yang bertujuan untuk memberi peringatan dan efek jera (*tankif*). Dalam konteks syar'i, *ta'zir* diterapkan sebagai sanksi atas kemaksiatan, yang tidak termasuk dalam kategori kejahatan yang secara eksplisit disebutkan dalam al-Qur'an dan al-Hadits, seperti hukuman *had/hudud*, *qishash-diyat*, dan *kafarat*. Jenis hukuman *ta'zir* ditentukan melalui proses peradilan yang sepenuhnya berada di bawah kewenangan hakim. Hakim memiliki otoritas untuk memutuskan bentuk hukuman yang akan dijatuhkan, seperti penjara, pengasingan, cambuk, atau bahkan hukuman mati, dengan mempertimbangkan tingkat kerugian (*mudharat*) yang ditimbulkan oleh tindakan pelaku.<sup>24</sup>

Asy-Syaikh as-Sa'adi dalam *Al-Muntaqa Syarh Al-Muwaththa'* jilid 6 yang dikutip oleh as-Sidawi dalam *Fiqih Kontemporer*,<sup>25</sup> menyatakan: "Setiap permasalahan yang muncul pada setiap zaman harus terlebih dahulu dipahami dengan jelas gambaran dan hakikatnya. Setelah itu, barulah permasalahan

---

<sup>23</sup> Gunawan, "Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah."

<sup>24</sup> Topo Santoso, *Membumikan Hukum Pidana Islam: Penegakan Syariat Dalam Wacana Dan Agenda* (Jakarta: Gema Insani, 2003).

<sup>25</sup> Abu Ubaidah Yusuf bin Mukhtar As-Sidawi, *Fiqih Kontemporer* (Gresik: Media Dakwah Al Furqon, 2013).

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

tersebut dapat dikembalikan kepada teks-teks syar'i dan kaidah-kaidah yang relevan." Dari penjelasan ini dapat disimpulkan bahwa untuk memutuskan hukum terhadap *cyber crime*, penting untuk memahami terlebih dahulu tindakan yang dilakukan oleh pelaku. Sebagai contoh, apabila pelaku terlibat dalam pencurian di dunia maya dengan cara-cara yang telah dipaparkan sebelumnya, pertanyaan yang timbul adalah apakah perbuatan tersebut memenuhi unsur-unsur dari *jarimah sirkah* (pencurian) dalam hukum pidana Islam sehingga pelaku dapat dijatuhi hukuman *hadd*?

Berbagai jenis *cyber crime* yang telah dibahas sebelumnya, fokus utama penulis adalah pada empat kategori yang paling sering ditemukan dalam praktik kejahatan dunia maya, yaitu pencurian, penipuan, pemerasan atau pengancaman, serta pelanggaran kesusilaan. Selanjutnya, penulis akan menguraikan secara ringkas keempat jenis kejahatan tersebut, yang sering kali menjadi modus operandi para pelaku *cyber crime*. Setelah mengidentifikasi jenis-jenis praktik yang dilakukan oleh pelaku, kemudian mengkaji korelasi antara tindak pidana tersebut dengan berbagai *jarimah* dan *uqubah* yang sesuai dalam kerangka hukum pidana Islam.

Dalam hal pencurian, para imam mazhab memiliki perbedaan pandangan mengenai *nisab* atau batas minimal nilai barang yang dicuri untuk dikenakan hukuman *hadd*. Imam Hanafi menetapkan *nisab* sebesar 1 dinar atau 10 dirham, sedangkan Imam Maliki, Syafi'i, dan Hanbali menetapkan *nisab* sebesar seperempat dinar atau 3 dirham. Selain itu, syarat bahwa barang harus disimpan di tempat yang terjaga juga menjadi pertimbangan penting, meskipun definisi pemeliharaan harta berbeda antar mazhab.<sup>26</sup> Dalam konteks *cyber crime*, pencurian data pribadi atau informasi rahasia yang dilakukan dengan sistem keamanan yang sah dapat memenuhi unsur pencurian menurut hukum Islam, sehingga jika syarat-syaratnya terpenuhi, dapat dikenai hukuman *hadd*, namun apabila tidak, pelaku akan dikenakan hukuman *ta'zir*, yaitu hukuman yang ditentukan oleh hakim sesuai dengan pertimbangan dan keadaan kasus yang bersangkutan.<sup>27</sup>

Penipuan merupakan tindakan berdusta yang diidentifikasi sebagai ciri perilaku munafik, sebagaimana dijelaskan dalam hadits dan ayat al-Qur'an.

---

<sup>26</sup> Syaikh al-'Allamah Muhammad bin 'Abdurrahman Ad-Damisyqi, *Fiqih Empat Mazhab*, ed. Irwan Kurniawan, trans. 'Abdullah Zaki Alkaf, 13th ed. (Bandung: Hasyimi, 2010).

<sup>27</sup> Muhammad Mawardi Djalaluddin et al., "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, <https://doi.org/10.22373/sjkh.v7i1.15101>.

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

Meskipun tidak ada *nash* eksplisit yang mengatur penipuan dalam konteks kejahatan dunia maya, penipuan digital tetap mendapatkan perhatian dalam kerangka hukum Islam. Oleh karena itu, untuk kejahatan penipuan yang terjadi melalui teknologi informasi, sanksi yang diterapkan adalah hukuman *ta'zir*, di mana hakim berwenang menentukan hukuman berdasarkan tingkat keparahan pelanggaran. Pemerasan dan pengancaman melibatkan pengambilalihan harta secara paksa tanpa dasar transaksi yang sah, dan dalam praktiknya, modus operandi ini menyerupai penodongan atau perampokan di dunia nyata. Demikian pula, pelanggaran kesusilaan dalam ruang digital, seperti pelecehan seksual *online*, merupakan bentuk kejahatan baru yang terus berkembang. Kedua jenis kejahatan ini umumnya tidak memenuhi syarat-syarat khusus untuk dikenakan hukuman *hudud* dalam hukum pidana Islam, sehingga sanksi yang diterapkan adalah hukuman *ta'zir*, yang disesuaikan dengan kondisi dan pertimbangan kasus oleh legislator dan hakim.<sup>28</sup>

Dengan demikian, dapat disimpulkan bahwa kejahatan dunia maya atau *cyber crime* menurut hukum pidana Islam tidak memenuhi kriteria untuk dikenakan sanksi *hudud*, mengingat terdapat syarat-syarat khusus yang tidak terpenuhi, seperti *nisab* dan perlindungan fisik terhadap objek yang dicuri dalam konteks *cyber crime*. Oleh karena itu, sanksi yang dikenakan kepada pelaku kejahatan dunia maya ini lebih cenderung berupa hukuman *ta'zir*.

Di Indonesia, kejahatan dunia maya telah menimbulkan dampak negatif signifikan, mulai dari kerugian finansial hingga permasalahan diplomatik. Untuk mengatasi hal ini, telah dilakukan upaya pencegahan seperti edukasi masyarakat mengenai pentingnya penggunaan kata sandi yang kuat dan pemahaman hak privasi, serta urgensi pembaruan sistem keamanan siber seiring kemajuan teknologi. Baik pemerintah maupun individu diharapkan rutin mengevaluasi keamanan kata sandi dan memantau aktivitas log untuk mendeteksi potensi ancaman, sehingga tindakan mitigasi dapat segera dilakukan.<sup>29</sup> Peningkatan kapasitas dan kompetensi aparat penegak hukum juga menjadi krusial agar tugas penegakan hukum terhadap tindak pidana komputer tidak membebani mereka secara tidak proporsional. Dalam konteks ini, revisi RUU ITE dan konsep

---

<sup>28</sup> Gunawan, "Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah."

<sup>29</sup> Hapsari and Pambayun, "Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis."

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

RUU KUHP memberikan kerangka kebijakan kriminalisasi kejahatan siber yang lebih adaptif terhadap tantangan hukum pidana masa depan.<sup>30</sup>

Nodeland & Morris<sup>31</sup> mengungkapkan bahwa bergaul dengan individu yang mendukung aktivitas kejahatan dunia maya dapat meningkatkan risiko keterlibatan dalam kejahatan ini secara signifikan, bahkan melebihi pengaruh keterampilan teknis semata. Maka dari itu, sangat penting untuk menjauhi lingkungan atau kelompok yang dapat memfasilitasi tindakan ilegal ini. Zhou et al.,<sup>32</sup> mengungkapkan bahwa anonimitas internet dapat memperberat proses identifikasi pelaku karena penyidik harus bergantung pada bukti digital, sehingga diperlukan strategi penanganan menyeluruh untuk mengatasi kendala-kendala tersebut.

Islam melarang segala bentuk perbuatan yang merugikan orang lain, baik secara fisik maupun nonfisik. Kejahatan dunia maya seperti penipuan, pencurian data, peretasan, dan penyebaran hoaks jelas bertentangan dengan nilai kejujuran, keadilan, dan amanah. Oleh karena itu, pendidikan moral dan akhlak Islami yang ditanamkan melalui keluarga, sekolah, dan masyarakat menjadi fondasi penting dalam membentuk perilaku etis, serta penguatan etika digital agar penggunaan teknologi tetap sesuai koridor syariat.<sup>33</sup>

Penanggulangan kejahatan dunia maya dalam hukum Islam diantisipasi melalui pendekatan *ta'zir*, yang memungkinkan hukuman disesuaikan dengan tingkat pelanggaran, serta penerapan prinsip *restorative justice* untuk pemulihan hak korban.<sup>34</sup> Selain itu, prinsip tanggung jawab kolektif dan pengawasan berbasis komunitas sesuai dengan *amar ma'ruf nahi munkar*, serta kolaborasi antara pemerintah dan lembaga berbasis nilai Islam, mendukung regulasi dan sistem keamanan digital yang efektif. Sanksi terhadap pelaku tidak hanya mencakup aspek hukum, tetapi juga dimensi moral dan spiritual melalui penegakan *taubat nasuha* (pertaubatan yang tulus) dan pembinaan keagamaan.

---

<sup>30</sup> Pansariadi and Soekorini, "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya."

<sup>31</sup> "A Test of Social Learning Theory and Self-Control on Cyber Offending," *Deviant Behavior* 41, no. 1 (2020): 41-56, <https://doi.org/10.1080/01639625.2018.1519135>.

<sup>32</sup> "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality."

<sup>33</sup> Ali Sodikin, "Legal, Moral, and Spiritual Dialectics in The Islamic Restorative Justice System," *AHKAM: Jurnal Ilmu Syariah* 21, no. 2 (2021): 357-78, <https://journal.uinjkt.ac.id/index.php/ahkam/article/view/22675>.

<sup>34</sup> Gunawan, "Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah"; Sodikin, "Legal, Moral, and Spiritual Dialectics in The Islamic Restorative Justice System."

### D. Kesimpulan

Hukuman untuk tindak pidana kejahatan dunia maya menurut hukum positif di Indonesia melalui UU ITE bervariasi, dengan ancaman maksimal berupa penjara hingga 10 tahun atau denda Rp10 miliar, tergantung jenis pelanggaran. Namun, undang-undang tidak secara eksplisit menetapkan hukuman minimal, memberikan hakim kebebasan dalam menentukan putusan berdasarkan konteks kasus. Dalam hukum pidana Islam, *cyber crime* tidak memenuhi kriteria sanksi *hadd* karena syarat-syarat seperti *nisab* dalam pencurian tidak terpenuhi. Oleh karena itu, hukuman dijatuhkan dalam bentuk *ta'zir*, yang memungkinkan hakim menyesuaikan sanksi dengan tingkat pelanggaran dan dampaknya. Kejahatan dunia maya menghadirkan tantangan besar dalam investigasi dan penegakan hukum, terutama karena anonimitas pelaku di dunia maya dan ketergantungan pada bukti digital. Kondisi ini menuntut strategi penanganan yang komprehensif, baik melalui penguatan regulasi maupun kolaborasi antara penegak hukum, pemerintah, dan masyarakat. Selain itu, penguatan nilai-nilai keislaman di masyarakat berperan penting dalam mencegah tindakan yang berpotensi melanggar hukum di dunia maya. Sinergi ini menjadi kunci untuk menciptakan sistem penanggulangan *cyber crime* yang efektif dan berintegritas.

### Referensi

- Ad-Damisyqi, Syaikh al-'Allamah Muhammad bin 'Abdurrahman. *Fiqih Empat Mazhab*. Edited by Irwan Kurniawan. Translated by 'Abdullah Zaki Alkaf. 13th ed. Bandung: Hasyimi, 2010.
- Alomar, Ahmad Mohamad, and Hassan Sami Alabady. "The Phenomenon of Cyber Bullying: Interpretation, Confrontation, and the Position of Islamic Law." *Journal of Namibian Studies: History Politics Culture* 34 (2023): 746-768. <https://doi.org/10.59670/jns.v34i.1123>.
- As-Sidawi, Abu Ubaidah Yusuf bin Mukhtar. *Fiqih Kontemporer*. Gresik: Media Dakwah Al Furqon, 2013.
- Creswell, John W., and J. David Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Edited by Helen Salmon, Chelsea Neve, Megan O'Heffernan, David C. Felts, and Amy Marks. 5th ed. Thousand Oaks, California: Sage Publications, Inc., 2018. <https://lcn.loc.gov/2017044644>.
- Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World'

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

- Policing and Law Enforcement.” *The Police Journal: Theory, Practice and Principles* 96, no. 4 (2023): 573–92. <https://doi.org/10.1177/0032258X221107584>.
- Djalaluddin, Muhammad Mawardi, Bulqia Mas’ud, Dedy Sumardi, Isnawardatul Bararah, and Kamus Kamus. “The Implementation of Ta’zīr Punishment as an Educational Reinforcement in Islamic Law.” *Samarah: Jurnal Hukum Keluarga Dan Hukum Islam* 7, no. 1 (2023): 399. <https://doi.org/10.22373/sjhk.v7i1.15101>.
- Gunawan, Hendra. “Tindak Kejahatan Cyber Crime Dalam Perspektif Fikih Jinayah.” *Jurnal El-Qanuniy: Jurnal Ilmu-Ilmu Kesyarahan Dan Pranata Sosial* 6, no. 1 (2020): 96–110. <https://doi.org/10.24952/el-qanuniy.v6i1.2473>.
- Hallaq, Wael B. *An Introduction to Islamic Law*. Cambridge: Cambridge University Press, 2009.
- Hapsari, Rian Dwi, and Kuncoro Galih Pambayun. “Ancaman Cybercrime Di Indonesia: Sebuah Tinjauan Pustaka Sistematis.” *Jurnal Konstituen* 5, no. 1 (2023): 1–17. <https://doi.org/10.33701/jk.v5i1.3208>.
- Irshad, Shareen, and Tariq Rahim Soomro. “Identity Theft and Social Media.” *IJCSNS International Journal of Computer Science and Network Security* 18, no. 1 (2018): 43–55. [http://paper.ijcsns.org/07\\_book/201801/20180106.pdf](http://paper.ijcsns.org/07_book/201801/20180106.pdf).
- Kaur, Gagandeep, Utkarsha Bonde, Kunjal Lalit Pise, Shruti Yewale, Poorva Agrawal, Purushottam Shobhane, Shruti Maheshwari, Latika Pinjarkar, and Rupali Gangarde. “Social Media in the Digital Age: A Comprehensive Review of Impacts, Challenges and Cybercrime.” In *Engineering Proceedings*, 6. Basel Switzerland: MDPI, 2024. <https://doi.org/10.3390/engproc2024062006>.
- Lee, So-Hyun, Ilwoong Kang, and Hee-Woong Kim. “Understanding Cybercrime from a Criminal’s Perspective: Why and How Suspects Commit Cybercrimes?” *Technology in Society* 75 (2023): 102361. <https://doi.org/10.1016/j.techsoc.2023.102361>.
- Marwan, Awaludin, Diana Odier-Contreras Garduño, and Fiammetta Bonfigli. “Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia.” *BESTUUR* 10, no. 1 (2022): 22. <https://doi.org/10.20961/bestuur.v10i1.59143>.
- Mejri, Mariem, Hakim Ben Othman, Basiem Al-Shattarat, and Kais Baatour. “Effect of Cultural Tightness-Looseness on Money Laundering: A Cross-Country Study.” *Journal of Money Laundering Control* 25, no. 2 (2022):

## Perbandingan Perspektif Hukum...

Zulfahmi,dkk...

- 414–26. <https://doi.org/10.1108/JMLC-03-2021-0025>.
- Nodeland, Brooke, and Robert Morris. "A Test of Social Learning Theory and Self-Control on Cyber Offending." *Deviant Behavior* 41, no. 1 (2020): 41–56. <https://doi.org/10.1080/01639625.2018.1519135>.
- Nurse, Jason R. C. "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit." In *The Oxford Handbook of Cyberpsychology*, edited by Alison Attrill-Smith, Chris Fullwood, Melanie Keep, and Daria J. Kuss, 662–90. Oxford: Oxford University Press, 2019. <https://doi.org/10.1093/oxfordhb/9780198812746.013.35>.
- Pansariadi, Rafi Septia Budianto, and Noenik Soekorini. "Tindak Pidana Cyber Crime Dan Penegakan Hukumnya." *Binamulia Hukum* 12, no. 2 (2023): 287–98. <https://doi.org/10.37893/jbh.v12i2.605>.
- Republik Indonesia. "Undang-Undang (UU) Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952)," 2024.
- Santoso, Topo. *Membumikan Hukum Pidana Islam: Penegakan Syariat Dalam Wacana Dan Agenda*. Jakarta: Gema Insani, 2003.
- Sarkar, Gargi, and Sandeep K. Shukla. "Behavioral Analysis of Cybercrime: Paving the Way for Effective Policing Strategies." *Journal of Economic Criminology* 2 (2023): 100034. <https://doi.org/10.1016/j.jeconc.2023.100034>.
- Sodiqin, Ali. "Legal, Moral, and Spiritual Dialectics in The Islamic Restorative Justice System." *AHKAM : Jurnal Ilmu Syariah* 21, no. 2 (2021): 357–78. <https://journal.uinjkt.ac.id/index.php/ahkam/article/view/22675>.
- Sugiyono. *Metode Penelitian Kuantitatif, Kualitatif, Dan R&D*. Cet. 26. Bandung: Alfabeta, 2017.
- Tegegn, Dagm Alemayehu. "The Role of Science and Technology in Reconstructing Human Social History: Effect of Technology Change on Society." *Cogent Social Sciences* 10, no. 1 (2024). <https://doi.org/10.1080/23311886.2024.2356916>.
- Zhou, You, Milind Tiwari, Ausma Bernot, and Kai Lin. "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality." *Asian Journal of Criminology* 19, no. 3 (2024): 419–39. <https://doi.org/10.1007/s11417-024-09436-y>.