Universitas Internasional Batam
Fakultas Hukum
Jl. Gadjah Mada, Batam, 29442, Indonesia
Phone : (0778) 743 7111 Ext, 140.
Email: admin_jlpt@gmail.com

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

CRIMINAL LIABILITY FOR DARK PATTERNS PRACTICES IN PERSONAL DATA PROCESSING

Yusuf Bagus Febrianto[1]*, Selamat Widodo[2], Yusuf Saefudin[3]*****
Faculty of Law, Universitas Muhammadiyah Purwokerto

Abstract

This study analyzes criminal liability arising from the use of dark patterns in the registration processes of digital platforms and applications, which frequently manipulate users into providing consent for the processing of their personal data without genuine understanding. Dark patterns are intentionally designed interface strategies that exploit visual, cognitive, and psychological mechanisms to influence user behavior, effectively eliminating freely given consent. The research examines the legal basis for imposing criminal liability under Indonesia's Personal Data Protection Law (Law No. 27 of 2022), the Electronic Information and Transactions Law, and the 2023 Criminal Code, while also evaluating the obstacles that hinder enforcement against such practices. Employing a normative legal research method with statutory, conceptual, and case approaches, the study demonstrates that dark patterns may satisfy the elements of criminal offenses, including intentionality, deception, and unlawful economic gain, allowing liability to be imposed on both individual actors and corporate entities. Analysis further reveals that enforcement remains limited due to the absence of an independent personal data protection authority, unclear standards regulating manipulative interface design, and low digital literacy among the Indonesian public. The study contributes to the ongoing transformation of Indonesia's legal framework, offering evidence-based insights for strengthening digital governance, ensuring accountability of data controllers, and reforming data protection policies to better safeguard individual rights in the rapidly evolving digital ecosystem.

Keywords: *dark patterns, criminal liability, personal data protection.*

A. Background

The rapid development of digital technology has transformed human life comprehensively, not only in terms of communication and information but also in ways of thinking, behaving, and interacting among individuals and institutions. The digital revolution has brought a fundamental shift in the global economic structure, where the digital economy has become the backbone of economic growth in many countries, including Indonesia. In this context, digital transformation creates vast opportunities for business innovation, operational efficiency, and accessibility to both public and private services. However, on the other hand, these changes also present complex challenges, particularly regarding ethics, privacy, and data security. The massive use of digital technology has turned data into a highly valuable commodity, creating an urgent need for legally and ethically regulated data governance. The internet functions not only as a medium for delivering information but also as a tool for processing, exchanging, and

[1] Corresponding Author: * yusufbagus.febrianto@gmail.com
[2] ** swidodo.sh@gmail.com
[3] *** yusufsaefudin12@ump.ac.id

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

storing data in digital form that is fast, efficient, and global in scale, thereby expanding the scope and impact of every digital activity carried out by individuals and institutions[4].

Protection of the right to privacy is an integral part of human rights guaranteed by the constitution. In Indonesia, Article 28G paragraph (1) of the 1945 Constitution explicitly states that every person has the right to protection of their personal integrity, family, honor, dignity, and property under their authority. This right includes protection from threats that may interfere with an individual's freedom to act or not act according to their fundamental rights. In the digital context, the right to privacy includes the right to control, manage, and safeguard personal data from unauthorized collection, use, or dissemination[5]. To strengthen such protection, the Indonesian government enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) on October 17, 2022. The PDP Law serves as a comprehensive legal framework regulating all aspects of personal data processing, from collection, processing, and storage to deletion, ensuring that individual rights over their personal data are preserved amid the accelerating pace of digitalization.

The PDP Law establishes several fundamental principles that must be complied with by all data processors, whether state administrators, legal entities, or individuals. These principles include legal certainty, usefulness, precaution, balance between personal and public interests, confidentiality, and accountability. This means that any processing of personal data must be carried out lawfully, transparently, and responsibly, taking into account both the benefits obtained and the potential risks. Moreover, the PDP Law emphasizes the importance of free, specific, and well-informed consent from data subjects as a key requirement for data processing. However, in practice, many violations of this principle occur, particularly through the use of manipulative techniques known as dark patterns. Dark patterns are deliberately designed digital interfaces that mislead users into giving consent without fully understanding the consequences, for example, a large, prominent "agree" button contrasted with a hidden or difficult-to-find "disagree" option. This phenomenon indicates a serious gap in the implementation of data protection, where technology is used to undermine individual autonomy[6].

Technological advancements in the era of the Industrial Revolution 4.0 and 5.0 have enabled large-scale, real-time collection, processing, and dissemination of data with wide scope and high complexity. Innovations such as artificial intelligence (AI), big data analytics, and machine learning allow digital service providers to analyze user behavior, predict needs, and target advertisements with precision. Although these innovations offer significant benefits in terms of efficiency and service personalization, their use also poses major risks to individual privacy and autonomy. Many companies engage in mass data collection without considering whether such data is truly necessary, operating under the assumption that all data may be valuable in the future. This approach potentially violates the principles of proportionality and purpose limitation set out in the PDP Law.

---

4 Ahmad Ihsan Amri and Y A Triana Ohoiwutun, "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana," *Opinia de Journal* 4, no. 1 (2024): 13–26.

5 Olga Salsabila Kiasatina, Laely Wulandari, and Idi Amin, "Perlindungan Hukum Terhadap Pengguna Pinjaman Online Yang Menjadi Korban Tindak Pidana Pencurian Data Pribadi," *Jurnal Parhesia* 3, no. 1 (2025): 1–15.

6 Ismaidar and Rifqi Fairuz Ula, "Pertanggungjawaban Pidana Korporasi Terhadap Kebocoran Data Pribadi Konsumen Dalam Perspektif Hukum Pidana Siber Di Indonesia," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 3 (2025): 44–51.

The new Criminal Code (KUHP) under Law Number 1 of 2023 provides detailed regulations on criminal acts and criminal liability. Article 12 paragraph (1) of the KUHP states that a criminal act is an action that is punishable under criminal law. Meanwhile, Article 36 paragraph (1) establishes that individuals can only be held liable for criminal acts committed intentionally or negligently. In the context of dark patterns, digital service providers who intentionally design manipulative interfaces may fall under the category of criminal acts due to the element of intent to mislead users[7].

The fundamental principles of criminal law emphasize the importance of fault (schuld) and accountability (toerekeningsvatbaarheid). In the practice of dark patterns, data controllers or corporations as legal subjects can be held criminally liable if they are proven to have fulfilled the elements of an intentional criminal act. The 2023 KUHP recognizes corporations as subjects of criminal acts, as stipulated in Article 45 paragraph (1), which states that corporations, including limited liability companies, foundations, cooperatives, and other business entities, may be held liable. This underscores that criminal liability is not limited to individuals but may also be imposed on legal entities involved in dark patterns practices[8].

Processing personal data through manipulative means violates fundamental data protection principles emphasizing transparency, openness, and valid consent. Under the PDP Law, consent is deemed valid when given freely, specifically, informed, and unambiguously. However, dark patterns essentially eliminate such freedom because user consent is obtained through psychological manipulation. In criminal law, this condition may constitute a form of deception as regulated in Article 20 letter (d) of the KUHP, which includes inducing another person to commit a criminal act through deception.

Indonesia ranks eighth among the ten countries with the largest data breaches in the world, with 94.22 million leaked data records, indicating the high vulnerability of Indonesia's data protection systems. This phenomenon can be linked to the practice of dark patterns in personal data processing, namely manipulative strategies used by digital platforms to push users into giving consent without fully understanding the implications. Dark patterns often cause users to unknowingly surrender their personal data, which may subsequently be misused or even lead to large-scale data breaches. Thus, Indonesia's position on this list not only indicates weak cybersecurity but also reflects the tangible impact of manipulative practices in personal data management that have not been fully anticipated by regulations or public awareness[9].

Personal data is a fundamental aspect of the right to privacy. As stated by Westin in Privacy and Freedom, the right to privacy is each individual's claim to determine when, how, and to what extent information about themselves is communicated to others. In the practice of dark patterns, users lose control over their personal information because the consent they provide does not stem from full awareness. Therefore, dark patterns not only violate the right to privacy but also undermine principles of justice in criminal law[10].

---

7 Fransiscus Xaverius Watkat, Muhammad Toha Ingratubun, and Adelia Apriyanti, "Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana Di Indonesia," *Jurnal Hukum Ius Publicum* 5, no. 1 (2024): 153–75, https://doi.org/10.55551/jip.v5i1.83.

8 Watkat, Ingratubun, and Apriyanti.

9 Adi Ahdiat, "Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar," 2024, https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar.

10 Amri and Ohoiwutun, "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana."

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

From the perspective of criminal law theory, criminal liability aims to uphold legal norms and provide protection to society. The new Criminal Code (KUHP) regulates the purposes of punishment in Article 51, namely preventing criminal acts, rehabilitating offenders, resolving conflicts, and restoring social balance. Dark patterns practices clearly generate conflict between data controllers and data subjects, as they involve violations of honesty and transparency principles. Therefore, imposing criminal liability for dark patterns aligns with the stated purposes of punishment in the KUHP[11].

The theoretical foundation of this reasoning is rooted in corporate criminal liability and the doctrine of vicarious liability, which place corporations as legal subjects that can be held accountable for actions carried out by individuals acting for and on behalf of the corporation. According to Moeljatno, criminal liability includes an individual's ability to bear legal consequences of their actions if committed with fault (*schuld*). In the corporate context, such fault may be projected onto managers or controllers who determine company policies[12].

(Barda Nawawi Arief, 2018) explains that criminal responsibility in modern law is not only individual but also collective and functional, applying to those who hold strategic positions in determining corporate policy directions. This theory emphasizes the concept of the "functional perpetrator," namely a person who plays a decision-making role that leads to the commission of a criminal act, even if they do not carry out the act directly[13].

This is relevant to dark patterns practices because such strategies are often designed as corporate policies aimed at increasing profits by exploiting personal data. In their most common form, dark patterns are digital interface design techniques that psychologically manipulate users into making decisions contrary to their free will, such as granting excessive data access permissions, enrolling in automatic subscriptions, or making cancellation difficult. These practices do not arise spontaneously but are the result of strategic planning that has undergone economic benefit analysis and legal risk assessment by corporate management teams. In many cases, legal teams and business teams participate in designing or approving these techniques, indicating collective intent and planning. Therefore, criminal liability can be directed not only at technical implementers but also at those who give orders and profit from the practice, as they contribute to building a corporate culture that prioritizes data exploitation over digital ethics and user rights.

The application of Article 54 of the KUHP in dark patterns cases also allows judges to impose sanctions that are proportional and just, based not only on the act committed but also on the social, economic, and moral context behind the act. For example, a giant technology corporation using dark patterns to expand its global user base may have far greater financial and technical capacity than conventional offenders; therefore, criminal sanctions should reflect their ability to improve systems and provide appropriate restitution to victims. Judges may also consider whether the conduct was systematic or sporadic, whether efforts were made to conceal the practice from the public, and the extent to which the corporation ignored ethical industry standards or data protection

[11] Amri and Ohoiwutun.
[12] Moeljatno, *Principles of Criminal Law* (Jakarta: Rineka Cipta, 2015).
[13] Ayu Efritadewi, *Criminal Law Module*, vol. 1 (Riau Islands: UMRAH Press, 2020).

regulations. By including these considerations, court decisions can become instruments for encouraging a transformation toward more responsible corporate digital practices[14].

Additionally, dark patterns may be associated with the concept of fraud, as they contain elements of deception and manipulation to gain profit. In criminal law, misleading acts conducted with the intent to obtain consent from another party for a particular action may constitute a punishable offense. The 2023 KUHP affirms that any person who induces another to commit a criminal act through deception may be punished (Article 20 letter d). This provision can serve as a normative basis for prosecuting dark patterns practices[15].

The enactment of the new KUHP is an important milestone in realizing national criminal law aligned with the values of Pancasila, human rights, and the needs of modern society. Within this framework, personal data protection through a criminal law approach becomes highly relevant, considering that personal data today is not only related to privacy rights but also concerns national security, economic stability, and digital sovereignty. Dark patterns that erode public trust in digital systems may be viewed as a serious threat requiring criminal law intervention[16].

Thus, criminal liability for dark patterns practices in personal data processing is an issue that cannot be overlooked. Philosophically, it relates to the protection of human rights; juridically, it has a foundation in the 2023 KUHP and the PDP Law; and sociologically, it arises from society's need for protection against harmful manipulative practices. This background shows that the discourse on dark patterns is not merely about technology and ethics but also concerns criminal law enforcement that demands certainty, justice, and real protection for every individual as the owner of personal data**.**

B. Identified Problems

Based on the background outlined above, the research questions are as follows:

1. What is the criminal liability for dark patterns practices in the registration process on digital platforms/applications?
2. What are the obstacles to law enforcement against dark patterns practices that meet the criteria for criminal elements in Indonesia?

C. Research Methods

The study employs a normative legal research method, focusing on the analysis of legal norms found in legislation, legal doctrines, and jurisprudence, as this prescriptive approach is most suitable for examining criminal liability in manipulative dark patterns practices involving personal data misuse. Using the statute approach, the research analyzes key provisions in Law No. 1 of 2023 on the Criminal Code (KUHP) and Law No. 27 of 2022 on Personal Data Protection (PDP Law) to interpret elements of criminal acts, intent, negligence, and the intersection between the two laws. A conceptual approach is also applied to explore doctrines such as mens rea, actus reus, manipulation, and deception through scholarly literature at the national and international levels. Additionally, the case approach examines national and international instances of dark

[14] Ismaidar and Ula, "Pertanggungjawaban Pidana Korporasi Terhadap Kebocoran Data Pribadi Konsumen Dalam Perspektif Hukum Pidana Siber Di Indonesia."
[15] Ismaidar and Ula.
[16] Aditya, Komang Masya Surya, and I Gusti Ngurah Nyoman Krisnadi Yudiantara, "Analisis Kriminologi Dalam Tindak Pidana Pencurian Data Pribadi Di Era Digital," *Jurnal Media Akademik* 3, no. 2 (2025): 6.

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

patterns use to assess legal application, evidentiary challenges, and judicial reasoning. The research uses primary, secondary, and tertiary legal materials, including KUHP, the PDP Law, academic publications, legal encyclopedias, and credible reports, collected through library research and documentation. Data are analyzed qualitatively using content analysis, involving data reduction, categorization, and normative interpretation through legal hermeneutics to identify themes, legal gaps, and the adequacy of current norms. The study concludes with prescriptive recommendations, including potential expansion of criminal provisions in the KUHP, strengthening sanctions in the PDP Law, and the need for more specific regulations on digital interface design. Integrating statute, conceptual, and case approaches, the research aims to construct a systematic, evidence-based argument to support future legal policy in addressing digital-era challenges**.**

D. Research Findings and Discussions

Criminal Liability for Dark patterns Practices in the Registration Process on Digital Platforms/Applications

Dark patterns are a form of manipulation in user interface design that are intentionally crafted to mislead or pressure users into making decisions that do not align with their true intentions or preferences. The interface, as a medium of interaction between humans and computer systems, should ideally be designed to facilitate easy understanding and effective system operation. However, in practice, many digital platforms exploit interface design for commercial gain, particularly in the context of collecting and processing personal data. Dark patterns operate by leveraging human cognitive processes, particularly System 1, rapid, intuitive, and impulsive decision-making, rather than System 2, which is more rational, reflective, and mentally effortful. By manipulating user conditions through techniques such as framing effects and anchoring, interface designers can unfairly influence user choices. As a result, users often give consent to the use of their personal data without fully understanding the consequences, as the process occurs automatically and unconsciously[17].

Dark patterns fundamentally contradict core principles of digital ethics, especially transparency, honesty, and user autonomy. The primary purpose of these techniques is not to educate or empower users, but to manipulate them into acting in the interests of data controllers, such as technology companies or digital service providers. Unlike conventional marketing, which aims to influence preferences through honest and open persuasion, dark patterns distort the decision-making process by creating illusions of choice, confusing users, or hiding options that may not benefit the company. For example, using an extremely small or hidden “Reject” button while making the “Accept” button prominent and easy to click is a common form of dark patterns that exploits visual and cognitive biases. In this way, users are unknowingly pushed toward options that benefit the company, even when they want to protect their privacy. Such practices not only erode public trust in digital platforms but also threaten human rights, particularly the right to privacy and personal autonomy[18].

---

[17] Ampuan Situmeang, Nadia Carolina Weley, and Hari Sutra Disemadi, “Kepastian Pertanggungjawaban Hukum Pidana Korporasi Atas Penyalahgunaan Data Pribadi Di Indonesia,” *Proceedings Series on Social Sciences \& Humanities* 23 (2025): 8–15, https://doi.org/10.30595/pssh.v23i.1544.

[18] Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, and Muhammad Fadly Nasution, “Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

Legally, the use of dark patterns clearly violates the principle of valid consent as regulated in various international data protection frameworks. In the European Union, the General Data Protection Regulation (GDPR) requires consent to be freely given, specific, informed, and unambiguous. This means that users must genuinely understand what they are agreeing to and must have complete freedom to accept or refuse without pressure. In the United States, the California Consumer Privacy Act (CCPA) similarly emphasizes transparency and user control over personal data. However, despite the strictness of these regulations, violations continue to occur as many companies exploit interface design loopholes to obtain consent that appears legally valid but is ethically questionable. In Indonesia, Law Number 27 of 2022 on Personal Data Protection (UU PDP) serves as an important legal foundation for protecting citizens' privacy rights. The law requires data controllers to obtain explicit consent from data subjects before processing personal data. Unfortunately, the UU PDP does not yet provide a clear definition of what constitutes valid consent or explicitly prohibit the use of dark patterns, leaving room for exploitation of user ignorance[19].

Amid the increasing use of digital platforms, especially in the e-commerce sector, dark patterns practices have become increasingly widespread and have caused real harm to consumers. Various forms of misleading interface designs, such as auto-renewal subscription buttons that are difficult to cancel, hidden fees appearing only at the final checkout stage, or persistent, disruptive notifications, have become part of business strategies that prioritize conversion over fairness. Research conducted by Markoni Tri Wahyu Pranoto, I Made Kanthika, and Joko Widarto revealed that such manipulative designs directly limit consumer autonomy in making free and informed decisions[20]. Furthermore, Johan Alfred Sarades Silalahi, Yuspika Yuliana Purba, and Muhammad Fadly Nasution found that many platforms obtain user consent for personal data processing through confusing interface designs, making the legal validity of such consent questionable[21]. This condition demonstrates that many digital business practices currently operate in a legal gray area, exploiting regulatory gaps to extract value from users without adequate transparency.

One of the root problems in addressing dark patterns in Indonesia is the absence of a clear taxonomy and regulatory framework. A taxonomy or classification of dark patterns types is essential to distinguish between design innovations aimed at improving user experience and manipulative practices deliberately created to deceive or pressure users. For example, notifications intended to increase user engagement may be considered legitimate marketing strategies, but if they appear excessively and are difficult to dismiss, they fall into the category of nagging, a type of dark patterns. Without a standardized and widely accepted taxonomy, it becomes difficult for regulators, law enforcement, and the public to identify and take action against harmful practices. The absence of specific regulations explicitly governing dark patterns also leaves consumers

Hukum Pidana Di Indonesia," *Jurnal Minfo Polgan* 14, no. 1 (2025): 604–13, https://doi.org/10.33395/jmp.v14i1.14810.

19 Agung Fajriansyah, Rospita Adelina, and Mompang L Panggabean, "Reformasi Hukum Pidana Di Era Digital: Analisis Terhadap KUHP Baru," *Jurnal Hukum Mimbar Justitia* 11, no. 1 (2025): 218–30.

20 Tri Wahyu Pranoto et al., "Pertanggungjawaban Pidana Pembocoran Data Pribadi," *Jurnal Cinta Nusantara* 2, no. 2 (2024): 30–45.

21 Silalahi, Purba, and Nasution, "Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia."

Journal of Law and Policy Transformation
Website : https://journal.uib.ac.id/index.php/jlpt | E-ISSN : 2541-3139
JLPT Vol 10, No. 2-December 2025

without adequate legal protection, allowing digital businesses to continue employing manipulative strategies without meaningful consequences[22].

Obstacles in Law Enforcement Against Dark patterns Practices That Meet Criminal Elements in Indonesia

The development of digital technology has brought significant consequences to the legal relationship between service providers and users. One prominent phenomenon is the practice of dark patterns, a strategy of interface design intentionally crafted to manipulate user choices so that they give consent they never truly intended. This manipulation appears in various forms, ranging from obscuring information and disguising choices to psychological pressure that directs users to surrender their personal data. This practice raises serious issues in criminal law, because although the term *dark patterns* is not explicitly mentioned in Indonesian regulations, it directly intersects with criminal law principles that protect freedom of will, honesty, and legal certainty in social relations[23].

Dark patterns designs take advantage of user interface (UI) elements that directly interact with users, making the interface a subtle yet effective tool of manipulation. A user interface is not merely a visual display of an application or website; it is a crucial bridge between humans and computer systems, translating human actions such as clicks, swipes, or taps into commands the machine can understand, while also presenting data back to the user in an accessible form. In this context, the UI plays a central role in shaping digital experience, determining how intuitive, convenient, and efficient a platform is. However, when UI design is used unethically, as in dark patterns cases, its function shifts from assisting users to controlling them in ways that undermine user autonomy. Such designs are not intended to simplify use but rather to steer, mislead, or pressure users into acting according to the platform provider's interests, often without the user's full awareness[24].

In digital interactions, UI significantly influences user perception, comprehension, and decision-making, making it impossible to overlook its importance. Well-designed UI can enhance productivity, strengthen trust, and create positive user experiences. However, when design principles are used manipulatively, the results contradict digital ethics and fairness. Dark patterns represent abuse of interface design, where elements such as buttons, text, colors, layout, and animations are strategically arranged to confuse, pressure, or entice users into specific actions, such as giving personal data, subscribing to services, or canceling subscription cancellations. These patterns often hide behind a neutral or friendly appearance, making it difficult for ordinary users to detect the manipulation. Thus, rather than serving as a mediator between humans and technology, the UI becomes an instrument of exploitation that undermines freedom of choice[25].

---

[22] Mahrus Ali et al., "Perbedaan Tindak Hukum Pidana Cyber Crime Menurut KUHP Lama Dengan KUHP Baru Tahun 2023," *Jurnal Lentera Ilmu* 1, no. 1 (2024): 119–27.

[23] I Nyoman Susipta, "Dark patterns Dalam Digital Marketing: Etika Dan Dampaknya Terhadap Loyalitas Konsumen," *International Journal of Economics and Management Research* 4, no. 1 (2025): 583–90, https://doi.org/10.55606/ijemr.v4i1.324.

[24] Glory Sylviana, Diah Pawestri Maharani, and Afrizal Mukti Wibowo, "Keabsahan Praktik Dark patterns Terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi Di Indonesia," *RechtJiva* 2, no. 1 (2025): 66–85.

[25] Asep Mahbub Junaedi, "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi," *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan* 5, no. 2 (2025): 247–57, https://doi.org/10.51878/knowledge.v5i2.5269.

The lack of regulatory clarity and the weakness of law enforcement have created conditions that allow serious violations related to dark patterns practices to persist both in Indonesia and internationally, illustrating how weak legal enforcement provides fertile ground for harmful digital manipulation. A prominent example is the €50 million fine imposed by the French data protection authority, CNIL, on Google in 2019 for violating the GDPR. CNIL found that Google used opaque interface designs, concealed essential information about data processing, and arranged consent options in ways that required users to undergo a complicated process to refuse. This clearly violated the principle of free and informed consent. In the United States, Google was again fined $9.5 million in 2022 for using dark patterns to continue tracking users' locations even after users explicitly disabled the tracking feature. In this case, the system technically displayed notifications requesting permission, but with confusing designs and unclear options, many users unknowingly allowed access. These cases show that even major companies intentionally exploit cognitive weaknesses and interface design to maximize data collection, despite harming users and violating the law[26].

In Indonesia, although no major dark patterns case has yet reached court or resulted in explicit legal punishment as in France or the United States, several similar incidents have occurred in the form of consumer rights violations and harmful digital service practices. Several telecommunications operators have received administrative sanctions from the government for automatically activating subscription SMS services and premium voting features that deduct user credit without explicit consent. Official data from the Indonesian Consumers Foundation (YLKI) recorded that telecommunications service complaints are the highest among all public complaints, peaking during the widespread phenomenon of automatic credit deduction[27]. This practice is a form of dark patterns because users are encouraged to press an "agree" button without understanding the hidden consequences of the service being activated. The harm experienced by Indonesian consumers is direct, as credit deductions occur without proper authorization and are often difficult to recover. These findings indicate that although Indonesia's legal framework is not as stringent as Europe's, dark patterns practices have already caused significant harm and urgently require more assertive legal action[28].

These cases serve as a stark warning that dark patterns are not merely unfriendly design choices but serious violations of human rights and digital democracy principles. They erode trust between users and service providers, weaken individual autonomy, and create power imbalances in the digital ecosystem. Without stricter regulations and consistent law enforcement, such manipulative practices will continue to evolve, especially as technology becomes more complex and society increasingly depends on digital services. In Indonesia, although the Personal Data Protection Law (UU PDP) is an important step forward, further implementing regulations are needed, particularly detailed guidelines on ethical interface design, explicit prohibitions on dark patterns, and strict sanctions for violations. Additionally, public education on privacy rights and digital literacy must be strengthened so that users can recognize and resist these manipulative

[26] Junaedi.

[27] Detiknews, "SMS Credit Theft Dominates Consumer Complaints to YLKI," 2011, https://news.detik.com/berita/d-1737205/sms-pencurian-pulsa-dominasi-pengaduan-konsumen-ke-ylki.

[28] Rohmah Dwi Cahyaningsih et al., "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia Dan Malaysia," *Abdurrauf Science and Society* 1, no. 4 (2025): 800–811, https://doi.org/10.70742/asoc.v1i4.283.

practices. Only through a holistic approach involving legal frameworks, technological integrity, and public awareness can we ensure that the digital environment remains fair, transparent, and respectful of individual rights[29].

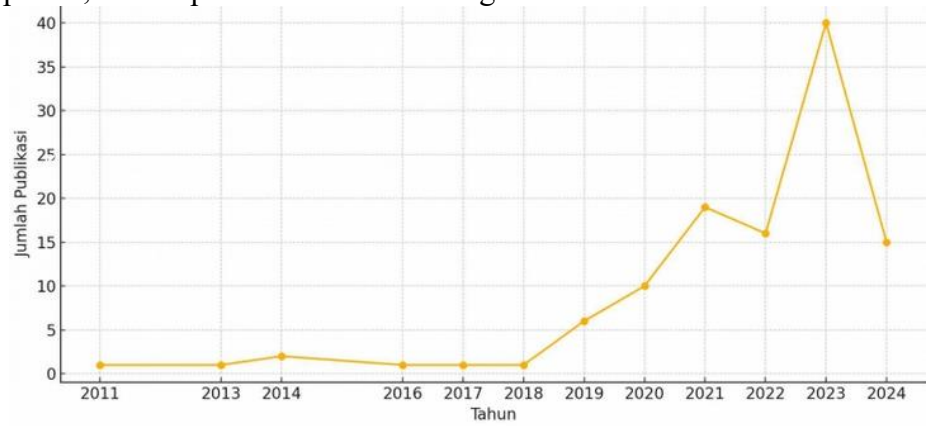

figure 1. Trends in Dark Patterns Case Publications
Source: (Kompasiana, 2024)

Dark patterns cases, also known as "deceptive patterns," have increasingly become a massive phenomenon in recent years, particularly alongside the rapid acceleration of digital transformation across various sectors. The number of publications shows a significant upward trend since 2019, with a sharp increase in 2023 reaching 40 publications. This figure reflects the growing academic and public attention toward manipulative digital design practices that fundamentally aim to influence user behavior in unethical ways. This phenomenon did not emerge suddenly; rather, it is the result of the swift expansion of digital technology, especially during the COVID-19 pandemic, when economic and social activities shifted massively to the online sphere. This transition forced society to quickly adapt to digital platforms, often without adequate understanding of their rights, risks, and self-protection mechanisms within the digital ecosystem[30].

The rapid development of digital technology in Indonesia indeed brings many benefits, particularly in terms of efficiency, accessibility, and business innovation. However, behind these conveniences lies a serious gap related to the low level of digital literacy among the public. Data from the Indonesian Internet Service Providers Association (APJII) shows that internet penetration in Indonesia reached 79.5% in 2024, illustrating the extensive spread of digital technology across all segments of society. Nevertheless, the public's understanding of how to use technology wisely, critically, and safely remains extremely limited. This is reinforced by the Indonesian Digital Society Index (IMDI), which recorded a decline from 26.19 in 2023 to 25.66 in 2024, indicating that although digital access is increasing, society's capacity to use it productively and effectively is actually decreasing. This gap between access and literacy creates significant

[29] Muhammad Rizki Kurniarullah et al., "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi," *Jurnal Ilmiah Wahana Pendidikan* 19, no. 5 (2016): 1–23.

[30] Alwan Setiawan, "Dark patterns Pada Bisnis Digital: Murni Inovasi Atau Pelanggaran Regulasi," 2025, https://www.kompasiana.com/84_077_alwansetiawan2338/6856b7fe34777c4e39105a32/dark-pattern-pada-bisnis-digital-murni-inovasi-atau-pelanggaran-regulasi.

vulnerability, making consumers susceptible to manipulative practices such as dark patterns that are intentionally designed to exploit users' lack of understanding[31].

The absence of an independent supervisory authority specifically responsible for personal data protection has become one of the biggest obstacles in enforcing laws related to dark patterns in Indonesia. The Personal Data Protection Act (UU PDP) mandates the establishment of the Personal Data Protection Authority (OPDP) as an independent institution tasked with oversight, investigation, compliance audits, and law enforcement. However, as of 2025, the formal structure of OPDP has not yet been established, and all supervisory duties are still temporarily handled by the Ministry of Communication and Informatics (Kominfo).

This situation presents a serious issue because Kominfo is not an independent body; it is part of the executive branch with overlapping functions as regulator, industry supervisor, and enforcement authority. This position creates potential conflicts of interest when dealing with major digital companies that may have economic ties to the government. Without an independent authority separated from political and economic interests, law enforcement becomes weak, especially in major cases involving global technology companies that hold significant influence in the national digital ecosystem[32].

Furthermore, without OPDP, investigative mechanisms that should be independent, rigorous, and equipped with full authority become limited, often resulting in public complaints ending merely with administrative clarifications rather than firm sanctions against violators. The absence of a dedicated supervisory body also hampers the implementation of interface design audits, which are crucial for detecting dark patterns at an early stage. In countries with mature data-protection systems such as France, Germany, and the Netherlands, interface audits are a key mechanism for identifying digital manipulation; thus, its absence in Indonesia highlights the vulnerability of the current data-protection framework[33].

According to Lawrence M. Friedman's legal system theory, there are three main elements that determine the effectiveness of law enforcement: legal structure, legal substance, and legal culture. These elements can be used to explain why dark patterns practices in Indonesia remain untouched by criminal sanctions even though such manipulative activities meet the criteria for violating privacy rights and potentially constitute digital crimes. From the perspective of legal structure, law-enforcement agencies do not yet have specialized units to handle interface-design violations or digital manipulation crimes, which are invisible and intangible. Authorities tend to focus on conventional crimes such as murder, rape, and physical violence due to their high social urgency, making algorithmic and hidden digital crimes lower priority. The lack of investigative units capable of understanding manipulative digital-design patterns also leads to difficulties in assessing wrongdoing, measuring losses, or proving intent in interface designs utilizing dark patterns[34].

---

31 Setiawan.

32 Edo Kurniawan, Firganefi Firganefi, and Dona Reisa Monica, "Upaya Penanggulangan Korban Tindak Pidana Penyalahgunaan Data Pribadi Di Media Sosial," *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 1 (2025): 204–18.

33 Ladito R Bagaskoro Ardi Ferdian Ridayani et al., *Perkembangan Hukum Pidana Di Indonesia* (Kabupaten Serang: PT Sada Kurnia Pustaka, 2023).

34 Lonna Yohanes Lengkong et al., *Buku Ajar Hukum Pidana* (Jakarta: UKI Press, 2023).

From the perspective of legal substance, regulations on dark patterns have not been explicitly formulated in national legislation. Although the PDP Law contains principles of honesty, transparency, and data minimization, it does not detail specific manipulative design forms that are prohibited nor mandatory audit mechanisms required for electronic-system providers. The absence of a legal definition of dark patterns hampers law enforcement at the interpretive level, as investigators must link technically manipulative practices with broadly formulated legal norms. This regulatory gap creates a gray area often exploited by digital platforms to disguise interface manipulation as "design choice," even though it substantively removes users' autonomy when providing consent[35].

From the perspective of legal culture, the greatest challenge arises from the low public awareness of the importance of personal data protection. Many Indonesians still view personal data as something with little economic value or risk, even though various studies highlight that data is the "new oil" of the modern digital economy and a strategic commodity frequently traded without the owner's knowledge. The fragile nature of Indonesia's digital culture leads people to easily grant app permissions, ignore security notifications, and fail to understand the consequences of clicking allow, agree, or continue. This environment allows dark patterns to flourish, as digital crimes that are invisible and occur on a massive scale are often perceived as harmless, even though their impact can reach millions of users. In many cases, the harm only becomes apparent when data is misused for online fraud, identity theft, unauthorized marketing, or more serious forms of behavioral exploitation[36].

The phenomenon of dark patterns does not stand alone; rather, it is closely related to the rise of digital content and application architectures that encourage risky public behavior. Many criminal cases that have emerged in recent years are influenced by unhealthy digital consumption patterns, including exposure to extreme violence, pornography, uncontrolled live streaming, and online gambling advertisements that frequently appear through automatic pop-ups even when users have never accessed such content. This type of content display is part of dark patterns, particularly the obstruction and nagging patterns, in which applications push users toward accessing content they do not actually want to see[37].

The psychological impact is far from simple; children and adolescents exposed to violent and pornographic content are at higher risk of imitating such actions or experiencing deviant behavioral changes. Studies in digital psychology show that exposure to harmful content can trigger aggressiveness, moral desensitization, and distortion of social values, which ultimately contributes to the rise of real-world violence[38].

Digital platforms frequently design interfaces that force users to remain within the application through autoplay features, disproportionate push notifications, and

---

[35] Difla Nur Maulida, Arfan Kaimuddin, and M Fahrudin Andriyansyah, "Tindak Pidana Pencurian Data Pribadi Di Internet," *Dinamika* 30, no. 1 (2024): 9370–85.

[36] Ida Bagus Anggapurana Pidada et al., *Tindak Pidana Dalam KUHP* (Bandung: Penerbit Widina Bhakti Persada, 2022).

[37] Rizha Claudilla Putri, "Dark patterns Sebagai Bentuk Manipulasi Perilaku Konsumen Digital: Analisis Interdisipliner Terhadap Dampak Psikologis, Hukum, Dan Ekonomi Dari Praktik Desain Manipulatif Dalam Ekosistem E-Commerce Global," *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (2025): 1066–71, https://doi.org/10.31004/riggs.v4i2.611.

[38] Rohmatullah, *Hukum Pidana Modern Dan Progresif* (Kota Solok: PT MAFY Media Literasi Indonesia, 2023).

algorithmic recommendations that prioritize watch duration. When harmful content appears as part of the normal flow of using the application, users are placed in a vulnerable position because their decisions are influenced by non-neutral design. In several criminal cases reported in the media, offenders admitted to being inspired by certain videos or application features that facilitated access to harmful content. This condition demonstrates that dark patterns not only cause economic or privacy-related losses but also contribute to broader patterns of social deviation. The absence of strict interface regulations allows digital platforms significant freedom to shape public behavior through design engineering that influences decisions without users' awareness.

In international legal systems, developed countries have implemented administrative and financial sanctions for dark patterns practices, primarily through consumer and data protection authorities. In the Netherlands, the Authority for Consumers and Markets (ACM) implements guidelines requiring ethical interface design and prohibits the use of automatic consent buttons, default opt-in settings, or pathways that make refusal difficult. The ACM imposes fines on companies proven to violate these guidelines on the basis that interface manipulation constitutes a form of commercial dishonesty. This model can serve as a reference for Indonesia, especially because dark patterns require responses that are fast, flexible, and effective; therefore, administrative sanctions such as proportional fines are far more appropriate than purely criminal processes, which are lengthy and inefficient.

In the Indonesian context, appropriate sanctions for dark patterns violations may include turnover-based fines or penalties calculated based on the number of affected users, cessation of data processing activities, mandatory interface corrections, or temporary suspension of digital services. Turnover-based fines have proven effective under the GDPR and were applied by CNIL in imposing massive penalties on Google. Considering that dark patterns are typically implemented by large companies with significant economic resources, financial sanctions must be designed to create a deterrent effect rather than becoming a mere operational cost. Additionally, Indonesia must adopt periodic interface audit mechanisms that can detect manipulation before it causes widespread public harm. A combination of fines, mandatory interface improvements, and transparent data processing will form the foundation of a proportional and effective sanctioning system[39].

A proper national policy must prioritize the establishment of an independent Data Protection Authority (OPDP) with full authority over oversight and enforcement concerning personal data protection, ensuring that regulatory decisions are insulated from political or economic influence and conflicts of interest, particularly when engaging with major digital corporations. The government should implement regulations under the Personal Data Protection Law (UU PDP) that explicitly define dark patterns practices, set ethical standards for interface design, and mandate regular audits for digital platforms to verify compliance. Law enforcement agencies require specialized training in forensic technology and interface design to detect digital evidence that is conceptual and not immediately visible, enabling effective investigation and prosecution. Industry stakeholders must integrate privacy by design principles and fair interface design standards as compulsory norms in all application updates, fostering responsible corporate behavior. Findings from other jurisdictions, such as the €50 million sanction against

[39] Esa Arung Syuhada and Pramudya Fikri Ananta, "Perlindungan Data Pribadi Terhadap Tindakan Doxing Dalam Perspektif Hukum Pidana," *Jurhum: Jurnal Humaniora* 2, no. 1 (2024): 37–46.

Google by France's CNIL for opaque interface design, illustrate how proactive regulatory frameworks and empowered independent authorities can effectively deter manipulative digital practices. These observations reinforce the need for Indonesia to transform its regulatory policy, institutional structures, and enforcement mechanisms to address dark patterns comprehensively and protect individual rights in the digital ecosystem[40].

At the societal level, strengthening digital literacy must become a continuous national program. The public must understand that every button, consent page, and data access request carries legal, economic, and social consequences. Public campaigns on privacy rights, valid consent, and how to interpret digital information must be disseminated through schools, social media, and public institutions so that users gain the capacity to identify and resist dark patterns. A combination of regulatory reform, enhanced institutional capacity, improved industry standards, and community empowerment will establish a digital ecosystem in Indonesia that is more equitable, secure, and respectful of individuals' fundamental rights.

E. Conclusions

Criminal liability for dark patterns practices in the registration processes of digital platforms can be applied through the Personal Data Protection Law (UU PDP), the Electronic Information and Transactions Law (UU ITE), and the 2023 Criminal Code (KUHP 2023). Under the UU PDP, deceptive or coercive interface designs that force users into giving non-voluntary consent may be classified as actions that unlawfully obtain or collect personal data as regulated in Article 65, with criminal sanctions stipulated in Article 67. The UU ITE also regulates interface manipulation as a form of electronic information deception that harms users, as stated in Article 28(1), Article 35, and Article 36, accompanied by criminal sanctions under Article 45A. Meanwhile, the KUHP 2023 provides additional legal grounds through Article 492 concerning deceit (tipu muslihat) and Article 508 regarding corporate liability for providing false information. Nevertheless, the absence of a legal definition of dark patterns, limited institutional capacity of supervisory agencies, the suboptimal role of data protection authorities, and low public digital literacy pose significant obstacles to law enforcement, especially because manipulative design practices are technical in nature and difficult to prove.

From an ius constituendum perspective, Indonesia requires regulatory reform that explicitly regulates and prohibits dark patterns practices in order to provide legal certainty and facilitate enforcement. This reform includes the need to establish clear standards on permissible and prohibited UI and UX practices, particularly those related to consent, personal data collection, and choice architectures that can influence user decision-making. These standards must be accompanied by firm sanction mechanisms such as turnover-based administrative fines, mandatory design corrections, service functionality restrictions, or other measures for repeated violations. Such regulatory reforms are necessary to systematically prevent dark patterns practices and ensure that users are protected from digital manipulation that may undermine autonomy, privacy, and security within the national digital ecosystem.

[40] A P Wardana, "Hukum Pidana Dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber Di Era Digital Di Indonesia," *Pustaka Law Journal*, 2024, 20–25, https://ojs.pustakapublisher.com/index.php/plj/article/view/18.

REFERENCES

Aditya, Komang Masya Surya, and I Gusti Ngurah Nyoman Krisnadi Yudiantara. "Analisis Kriminologi Dalam Tindak Pidana Pencurian Data Pribadi Di Era Digital." *Jurnal Media Akademik* 3, no. 2 (2025): 6.

Ahdiat, Adi. "Indonesia Masuk 10 Negara Dengan Kebocoran Data Terbesar," 2024. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar.

Ali, Mahrus, Kevin, Husein Syarif Hidayatullah, Firda Elena Sari, Fifi Fitria Aulia Ababil, and Nora Nadilla. "Perbedaan Tindak Hukum Pidana Cyber Crime Menurut KUHP Lama Dengan KUHP Baru Tahun 2023." *Jurnal Lentera Ilmu* 1, no. 1 (2024): 119–27.

Amri, Ahmad Ihsan, and Y A Triana Ohoiwutun. "Analisis Perlindungan Data Pribadi Ditinjau Dari Aspek Sistem Peradilan Pidana." *Opinia de Journal* 4, no. 1 (2024): 13–26.

Cahyaningsih, Rohmah Dwi, Anis Fauzan, Saupi Hasbi, and Atik Winanti. "Kebijakan Hukum Pidana Dalam Penanggulangan Tindak Pidana Phising Dengan Undang-Undang Perlindungan Data Pribadi: Studi Perbandingan Indonesia Dan Malaysia." *Abdurrauf Science and Society* 1, no. 4 (2025): 800–811. https://doi.org/10.70742/asoc.v1i4.283.

Detiknews. "SMS Credit Theft Dominates Consumer Complaints to YLKI," 2011. https://news.detik.com/berita/d-1737205/sms-pencurian-pulsa-dominasi-pengaduan-konsumen-ke-ylki.

Efritadewi, Ayu. *Criminal Law Module*. Vol. 1. Riau Islands: UMRAH Press, 2020.

Fajriansyah, Agung, Rospita Adelina, and Mompang L Panggabean. "Reformasi Hukum Pidana Di Era Digital: Analisis Terhadap KUHP Baru." *Jurnal Hukum Mimbar Justitia* 11, no. 1 (2025): 218–30.

Ismaidar, and Rifqi Fairuz Ula. "Pertanggungjawaban Pidana Korporasi Terhadap Kebocoran Data Pribadi Konsumen Dalam Perspektif Hukum Pidana Siber Di Indonesia." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 3 (2025): 44–51.

Junaedi, Asep Mahbub. "Urgensi Perlindungan Data Pribadi Dalam Era Digital: Analisis Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi." *KNOWLEDGE: Jurnal Inovasi Hasil Penelitian Dan Pengembangan* 5, no. 2 (2025): 247–57. https://doi.org/10.51878/knowledge.v5i2.5269.

Kiasatina, Olga Salsabila, Laely Wulandari, and Idi Amin. "Perlindungan Hukum Terhadap Pengguna Pinjaman Online Yang Menjadi Korban Tindak Pidana Pencurian Data Pribadi." *Jurnal Parhesia* 3, no. 1 (2025): 1–15.

Kurniarullah, Muhammad Rizki, Talitha Nabila, Abdurrahman Khalidy, Vivi Juniarti Tan, and Heni Widiyani. "Tinjauan Kriminologi Terhadap Penyalahgunaan Artificial Intelligence: Deepfake Pornografi Dan Pencurian Data Pribadi." *Jurnal Ilmiah Wahana Pendidikan* 19, no. 5 (2016): 1–23.

Kurniawan, Edo, Firganefi Firganefi, and Dona Reisa Monica. "Upaya Penanggulangan Korban Tindak Pidana Penyalahgunaan Data Pribadi Di Media Sosial." *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora* 2, no. 1 (2025): 204–18.

Lengkong, Lonna Yohanes, Andree Washington H Sianipar, Adrianus Herman Henok, Radisman Saragih, and Petrus Irwan Panjaitan. *Buku Ajar Hukum Pidana*. Jakarta: UKI Press, 2023.

Maulida, Difla Nur, Arfan Kaimuddin, and M Fahrudin Andriyansyah. "Tindak Pidana Pencurian Data Pribadi Di Internet." *Dinamika* 30, no. 1 (2024): 9370–85.

Moeljatno. *Principles of Criminal Law*. Jakarta: Rineka Cipta, 2015.

Pidada, Ida Bagus Anggapurana, Juanrico Alfaromona Sumarezs Titahelu, Azhar Arrahman Nainggolan, Lestari Victoria Sinaga, Deassy J A Hehanussa, Margie Gladies Sopacua, Christina Bagenda, and others. *Tindak Pidana Dalam KUHP*. Bandung: Penerbit Widina Bhakti Persada, 2022.

Pranoto, Tri Wahyu, Markoni, I Made Kanthika, and Joko Widarto. "Pertanggungjawaban Pidana Pembocoran Data Pribadi." *Jurnal Cinta Nusantara* 2, no. 2 (2024): 30–45.

Putri, Rizha Claudilla. "Dark patterns Sebagai Bentuk Manipulasi Perilaku Konsumen Digital: Analisis Interdisipliner Terhadap Dampak Psikologis, Hukum, Dan Ekonomi Dari Praktik Desain Manipulatif Dalam Ekosistem E-Commerce Global." *RIGGS: Journal of Artificial Intelligence and Digital Business* 4, no. 2 (2025): 1066–71. https://doi.org/10.31004/riggs.v4i2.611.

Ridayani, Ladito R Bagaskoro Ardi Ferdian, Muhamad Romdoni, Febrianika Maharani Ahdiyatul Hidayah, Celine Endang Patricia Sitanggang, Jusnizar Sinaga, July Esther, Adwi Mulyana, et al. *Perkembangan Hukum Pidana Di Indonesia*. Kabupaten Serang: PT Sada Kurnia Pustaka, 2023.

Rohmatullah. *Hukum Pidana Modern Dan Progresif*. Kota Solok: PT MAFY Media Literasi Indonesia, 2023.

Rosyadi, Imron. *Hukum Pidana*. Surabaya: Revka Prima Media, 2020.

Setiawan, Alwan. "Dark patterns Pada Bisnis Digital: Murni Inovasi Atau Pelanggaran Regulasi," 2025. https://www.kompasiana.com/84_077_alwansetiawan2338/6856b7fe34777c4e39105a32/dark-pattern-pada-bisnis-digital-murni-inovasi-atau-pelanggaran-regulasi.

Silalahi, Johan Alfred Sarades, Yuspika Yuliana Purba, and Muhammad Fadly Nasution. "Analisis Yuridis Terhadap Mekanisme Perlindungan Data Pribadi Dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana Di Indonesia." *Jurnal Minfo Polgan* 14, no. 1 (2025): 604–13. https://doi.org/10.33395/jmp.v14i1.14810.

Situmeang, Ampuan, Nadia Carolina Weley, and Hari Sutra Disemadi. "Kepastian Pertanggungjawaban Hukum Pidana Korporasi Atas Penyalahgunaan Data Pribadi Di Indonesia." *Proceedings Series on Social Sciences \& Humanities* 23 (2025): 8–15. https://doi.org/10.30595/pssh.v23i.1544.

Susipta, I Nyoman. "Dark patterns Dalam Digital Marketing: Etika Dan Dampaknya Terhadap Loyalitas Konsumen." *International Journal of Economics and Management Research* 4, no. 1 (2025): 583–90. https://doi.org/10.55606/ijemr.v4i1.324.

Sylviana, Glory, Diah Pawestri Maharani, and Afrizal Mukti Wibowo. "Keabsahan Praktik Dark patterns Terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi Di Indonesia." *RechtJiva* 2, no. 1 (2025): 66–85.

Syuhada, Esa Arung, and Pramudya Fikri Ananta. "Perlindungan Data Pribadi Terhadap Tindakan Doxing Dalam Perspektif Hukum Pidana." *Jurhum: Jurnal Humaniora* 2, no. 1 (2024): 37–46.

Wardana, A P. "Hukum Pidana Dan Perlindungan Data Pribadi: Upaya Menanggulangi Kejahatan Siber Di Era Digital Di Indonesia." *Pustaka Law Journal*, 2024, 20–25. https://ojs.pustakapublisher.com/index.php/plj/article/view/18.

Watkat, Fransiscus Xaverius, Muhammad Toha Ingratubun, and Adelia Apriyanti. "Perlindungan Data Pribadi Melalui Penerapan Sistem Hukum Pidana Di Indonesia." *Jurnal Hukum Ius Publicum* 5, no. 1 (2024): 153–75. https://doi.org/10.55551/jip.v5i1.83.