E-ISSN: 2986-8351
AAFJ Accounting & Finance Journal

Vol. 3, No. 1 (2025), pp. 35-45

Beware of Cybercrime in Tax Reporting: Threats and How to Protect Yourself

Muh. Akbar Fhad Syahril*[1], Sadmir Karovic[2]
Email: akbar9.a9@gmail.com[*1]

Article Info

Article history:
Received 02 January – 2025
Revised 20 January – 2025
Accepted 29 January – 2025

Abstract

Information and communication technology development has brought significant changes to the taxation system, including the emergence of increasingly complex cybercrimes. This study aims to analyze the evolution of cybercrimes in the digital taxation system and the strategies and challenges in dealing with them. The method used is qualitative normative with a literature study approach. The study results indicate that cybercrimes in taxation include identity fraud, fake tax refund schemes, and international tax evasion, with significant financial impacts. Law Number 1 of 2024 concerning the Second Amendment to the UU ITE provides a more substantial legal basis but still requires harmonization with existing tax regulations. The handling strategy involves applying digital forensics, artificial intelligence, and international cooperation. The main challenge lies in the complexity of cybercrime, which continues to grow, and the need for more comprehensive regulations. This study concludes that a holistic approach is needed to strengthen rules, increase technological capabilities, and educate taxpayers to overcome taxation cybercrimes in the digital era.

Keywords:
Cybercrime; Digital Taxation; Digital Forensics; Artificial Intelligence; Regulatory Harmonization

DOI:
10.56341/aafj.v3i1.572

INTRODUCTION

The development of information and communication technology has brought significant changes in various aspects of life,[3] Including in the field of taxation. In their research, Sadmir Karović and Marina M Simović assert that "the development of information and communication technology has brought radical changes in all aspects of human life, including in the field of criminal law".[4] This statement is very relevant to taxation, where increasingly digitalized tax reporting opens up new opportunities for

[1]Law Faculty, Andi Sapada Institute of Social Sciences and Business, Parepare, Indonesia
[2]Law Faculty, Travnik University, Bosnia and Herzegovina
[3]Syahril, M. A. F. (2023). Hukum Informasi dan Transaksi Elektronik.
[4]Karović, S., & Simović, M. (2022). Krivičnopravni I Viktimološki Aspekt Maloljetničke Delinkvencije–Izazovi, Dileme. Društvene Devijacije, 7(1).

cybercriminals to carry out their actions. According to data from usafacts.org, in 2022, there were around 800,000 reported cyber incidents, with financial losses reaching $7 billion to $10 billion.[5,6] These figures show how serious the threat of cybercrime is, including in the context of taxation, reflecting a radical change in the crime landscape.

Companies and individuals preparing to file tax returns are prime targets for cybercriminals.[7] Opening an email or answering a phone call can put someone at risk of identity theft or tax return fraud.[8] This situation is exacerbated by the increasing sophistication of cyberattacks, which are aided by the adoption of artificial intelligence and large language models like ChatGPT, which allow for the creation of more legitimate-looking and convincing messages.

The Internal Revenue Service (IRS) has warned taxpayers about various fraudulent schemes, including fake notices of unclaimed tax refunds, fake W-2 wages, unemployment benefits, natural disasters, and ghost preparers.[9] This year, the IRS also warned of increased scams by individuals posing as trusted tax professionals or friends to trick taxpayers into submitting personal information.

Cybercrime in taxation is not limited to fraud against individuals but also involves more complex schemes, such as international tax evasion. This can include transfer pricing schemes, shifting profits to tax havens, and manipulating financial information related to special corporate relationships. These actions can be classified as tax crimes because they are carried out with the principle of dishonesty through falsifying information in tax payments and reporting.

The impact of cybercrime on taxation is significant. Member countries of the Organisation for Economic Cooperation and Development (OECD) have suffered huge losses due to tax fraud. Of all cases of digital money laundering crimes, tax fraud ranks first, with a total loss of US$222.697 billion.[10] In Indonesia, the most common cause of a tax fraud investigation is tax invoices not based on actual transactions.

Various countries have taken proactive steps to address this issue. The United States, for example, passed the Critical Infrastructure Cyber Incident Reporting Act in 2022.[11] The law aims to improve information sharing between the private and government sectors to strengthen national cyber defences. Meanwhile, Australia has

[5]Nadya Britton. (2024). Tax season is on its way and so is cybercrime: Cybersecurity considerations for tax firms. https://www.thomsonreuters.com/en-us/posts/tax-and-accounting/cybersecurity-considerations/. Diakses tanggal 29 Desember 2024

[6]USAFacts team. (2023). How many cyber-attacks occur in the US?. https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us/. Diakses tanggal 30 Desember 2024

[7]Vassilis Kontoglis. (2024). Tax Season Brings Rise in Cyber Crime. https://www.aafcpa.com/2024/01/30/tax-season-brings-rise-in-cyber-crime/. Diakses tanggal 31 Desember 2024

[8]Syahril, M. A. F., & Hasan, H. (2024). A Comparative Research on the Effectiveness of Progressive versus Proportional Tax Systems in Enhancing Social Justice. Administrative and Environmental Law Review, 5(2), 97-106.

[9]*Op.cit*

[10]Madani, L., Sofia, A., & Widarsono, A. (2024). The Influence of Cybersecurity Disclosure, Tax Risk, Reputation and Auditor Experience on Audit Quality. Jurnal Pendidikan Akuntansi & Keuangan, 12(2), 138-149.

[11]PWC. (2022). Cyber Breach Reporting to be Required By Law For Better Cyber defense.

implemented tax digital forensics through technologies such as Universal Forensic Extraction software to support criminal investigations.[12]

In Indonesia, the Directorate General of Taxes (DGT) has implemented digital forensics as a tool in the tax law enforcement process. Through digital forensics, every digital tax crime can be revealed because it will leave traces in the form of digital files and documents. However, the DGT's digital forensics procedures still use semi-digital methods and have not fully adopted modern digital technology, which can be an obstacle if taxpayers remove and erase digital goods records.

Faced with these challenges, there is an urgent need to develop more comprehensive and effective regulations to address cybercrime in the tax sector. Appropriate regulations can help build a fairer and more transparent tax system and ensure that taxpayers can fulfil their tax obligations in accordance with the provisions of the laws and regulations.[13]

Table 1. Previous Studies

Name	Title	Research result
Lutfi Madani	The Influence of Cybersecurity Disclosure, Tax Risk, Reputation and Auditor Experience on Audit Quality.[14]	Cyber Security Disclosure positively affects audit quality.
Chiarini & Marzano	The Role of Tax Digital Forensics through the Utilization of Big Data.[15]	Digital forensics can minimize digital tax crime.
Bellasio, Jacopo Silverback, Erik Leverett, Ireland Knack, Anna Quimbre, Fiona Blondes, Emma Louise Favaro, Marina Persi Paoli, Giacomo	The Future of Cybercrime in Light of Technology Developments.[16]	Emerging technologies pose new threats to cybersecurity.

Given the complexity and dynamics of cybercrime in taxation, further research on the effectiveness of regulation and implementation of digital forensic technology in dealing with digital tax crimes is urgently needed. This study will explore how integrating big data analytics and artificial intelligence can improve the ability of tax authorities to detect and prevent crime. Cyber tax: This study will also investigate the balance between effective law enforcement and taxpayer privacy protection in the digital era. Thus, this study is expected to contribute significantly to developing more

[12]Madani, L., Sofia, A., & Widarsono, A. (2024). The Influence of Cybersecurity Disclosure, Tax Risk, Reputation and Auditor Experience on Audit Quality. Jurnal Pendidikan Akuntansi & Keuangan, 12(2), 138-149

[13]*Ibid*

[14]*Ibid*

[15]Widya, A., & Suryani, Y. (2024). The Role of Tax Digital Forensic through the Utilization of Big Data Analytics in Indonesia. E-INVESTA: Jurnal Rumpun Ilmu Ekonomi dan Bisnis Islam, 1(1), 33-55.

[16]Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., ... & Persi Paoli, G. (2020). The future of cybercrime in light of technology developments

effective policies and strategies to combat cybercrime in the tax system and the digital era.

RESEARCH METHODS

This study uses a qualitative method that collaborates with a normative approach. This normative qualitative method focuses on an in-depth analysis of legal norms, laws and regulations, and legal theories relevant to the research topic.[17] This approach allows researchers to study legal aspects comprehensively through literature studies, using secondary data from primary, secondary, and tertiary legal materials.[18] Data analysis is carried out qualitatively, where researchers describe the data systematically and logically to produce a deep understanding of the legal problems being studied.

The research flow in this method begins with identifying the problem and formulating research questions. Furthermore, the researcher collects data through a comprehensive literature study. The next stage is data analysis, where the researcher categorizes, systematizes, and interprets the data obtained. This process is followed by drawing conclusions and compiling recommendations based on the analysis results. The Research Flow is as follows:

Identification of problems
↓
Formulation of Research Questions
↓
Data Collection (Literature Study)
↓
Qualitative Data Analysis
↓
Drawing Conclusions
↓
Article Writing

RESULTS AND DISCUSSION

The Evolution of Cybercrime in Digital Taxation Systems

The evolution of cybercrime in the digital tax system has reached an alarming level of complexity, reflecting the rapid development of information and communication technology. The digitization of tax reporting, initially designed to increase efficiency and accuracy, has become a new arena for cybercriminals. Data from usafacts.org shows that 2022 there were around 800,000 reported cyber incidents, with financial losses reaching $7 billion to $10 billion.[19] This figure confirms how serious

[17]Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). Metode penelitian hukum. CV. Gita Lentera

[18]Rio Christiawan. (2023). Membaca Ulang Eksistensi Teori Pada Penelitian Normatif. https://www.hukumonline.com/berita/a/membaca-ulang-eksistensi-teori-pada-penelitian-normatif-lt64f99dc2f2924/. Diakses tanggal 31 Desember 2024

[19]Rahayu, S. K. Keamanan Digital dalam Audit Pajak. Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance.

the threat of cybercrime in the tax context is, demanding immediate attention and action from the relevant authorities.

Identity fraud in the context of taxation has emerged as one of the most prominent forms of cybercrime. Criminals exploit vulnerabilities in digital systems to steal taxpayer identities and use them for various illegal purposes. The severity of this issue is exemplified by the leak of 6 million NPWP (Nomor Pokok Wajib Pajak or Tax Identification Number) data by hacker Bjorka in September 2024, which involved data from high-ranking state officials, including President Joko Widodo, his children, and several ministers.[20.21]

This incident starkly illustrates the vulnerability of tax data security systems. The leaked data included sensitive information such as names, national identity numbers (NIK), NPWP, addresses, emails, phone numbers, dates of birth, and tax office details.[22] The data was reportedly being sold for US$10,000 (approximately 160 million rupiah),[23] highlighting the potential for financial exploitation.

The impact of such breaches extends beyond individual privacy concerns. According to the U.S. Government Accountability Office, hundreds of thousands of taxpayers face serious problems due to identity theft, even though they represent a small percentage of the total tax returns filed.[24] In the United States, it's estimated that the IRS could issue about $26 billion in fraudulent tax refunds resulting from identity theft over a five-year period.[25]

To address these growing concerns, Indonesia has taken legislative action. The Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik has been enacted to strengthen online privacy protection.[26] This law aims to maintain a clean, healthy, ethical, productive, and fair digital space in Indonesia.[27]

Key provisions of this law include:[28]

1. Enhanced protection of personal data in electronic systems.
2. Stricter regulations on the use and processing of personal data.
3. Increased responsibilities for electronic system operators in safeguarding user data.

These legislative measures are expected to help prevent cases similar to the Bjorka incident and improve overall cybersecurity in Indonesia's digital landscape. However, as cybercriminals continue to evolve their tactics, ongoing vigilance and

---

[20]Nina Susilo, Mawar Kusuma Wulan. (2024). When the President's and His Family's and Ministers' Data is Leaked and Sold. https://www.kompas.id/baca/english/2024/09/23/en-ketika-data-presiden-keluarganya-dan-para-menteri-dijual. Diakses 25 Januari 2025

[21]Wibi Pangestu Pratama. (2024). Data Ditjen Pajak Diduga Bocor, Ada NPWP Jokowi, Gibran, Kaesang, hingga Sri Mulyani. https://ekonomi.bisnis.com/read/20240918/259/1800454/data-ditjen-pajak-diduga-bocor-ada-npwp-jokowi-gibran-kaesang-hingga-sri-mulyani. Diakses 27 Januari 2025

[22]*Op.cit*

[23]*Ibid*

[24]James R. White. (2011). Taxes and Identity Theft Status of IRS Initiatives to Help Victimized Taxpayers. United States Government Accountability Office

[25]Megumi Kashiwagi.(n.d). Problem of Identity Theft and Fraudulent Tax Refunds in the United States: Considering the Possible Developments Following a Future Consumption Tax Increase and Introduction of the Social Security and Tax Number System. The Canon Institute for Global Studies

[26]*Vide* Undang-Undang Nomor 1 Tahun 2024 Tentang P-erubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

[27]*Ibid*

[28]Nabila, L., & Setianingrum, R. B. (2024). Analisis Perlindungan Data Pribadi bagi Pengguna E-commerce Menurut Perspektif Hukum di Indonesia. *Media of Law and Sharia*, *6*(1), 1-17.

adaptive security measures will be crucial in protecting taxpayer identities and maintaining the integrity of the tax system.

Fake tax refund schemes have evolved into increasingly sophisticated modus operandi. The Internal Revenue Service (IRS) has issued warnings about fraud schemes, including counterfeit notices of unclaimed tax refunds and fake Form W-2 wages.[29] Adopting artificial intelligence and large language models such as ChatGPT has further exacerbated the sophistication of these cyberattacks, which allows for the creation of more legitimate-looking and convincing fraudulent messages. The latest UU ITE has added Articles 27A and 27B, which specifically regulate the spread of false information and threats of violence, which can be applied in the context of online tax fraud.

Complex international tax avoidance is a challenge in the digital era. Transfer pricing schemes and profit shifting to tax havens are increasingly difficult to detect due to perpetrators' ability to hide their digital footprints. The "Panama Papers" phenomenon and the "Double Irish Dutch Sandwich" scheme used by multinational companies illustrate how digital technology is used for large-scale tax avoidance. The latest UU ITE has added provisions on international electronic contracts, which can help in dealing with cross-border tax avoidance cases.

The financial impact of cybercrime on the tax system is significant. OECD member countries have suffered huge losses from tax fraud, with total losses reaching US$ 222.697 billion from digital money laundering crimes. The most common tax fraud investigation case in Indonesia is a tax invoice that is not based on actual transactions.[30] The Gayus Tambunan case is a real example of how cybercrime can synergize with corruption in the tax system. It involves abuse of authority and manipulation of tax data that costs the state hundreds of billions of rupiah.

Various countries have taken proactive steps to address these challenges. In 2022, the United States passed the Cyber Incident Reporting for Critical Infrastructure Act to improve information sharing between the private sector and the government. Australia has implemented digital tax forensics through technologies such as Universal Forensic Extraction software. In Indonesia, the Directorate General of Taxes (DJP) has implemented digital forensics in the tax law enforcement process, although it still uses semi-digital methods that need to be improved.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik significantly strengthens the fight against cybercrime, including in the context of digital taxation. The addition of Article 13A, which regulates the services of Electronic Certification Providers, such as electronic signatures, digital identities, and website authentication, provides a clearer legal basis for improving the security of electronic transactions.[31] In the taxation system, electronic signatures and digital identities can ensure the validity and authenticity of taxpayer data, thereby reducing the risk of identity forgery or data manipulation in online tax reporting. In addition, website authentication helps taxpayers avoid fake sites often used in phishing attacks. With this

[29]Rahayu, S. K. Keamanan Digital dalam Audit Pajak. Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance.

[30]Maris, A. W. (2024). Analisis Yuridis Tindak Pidana Perpajakan sebagai Salah Satu Modus Operandi Tindak Pidana Korupsi di Indonesia. Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik, 1(3), 197-206.

[31]*Vide* Pasal 13 A Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

arrangement, the digital-based taxation system can be more secure and reliable, encouraging more taxpayers to take advantage of efficient online services.

On the other hand, adding the authority of Civil Servant Investigators (PPNS) to investigate cyber crimes also has significant implications for law enforcement in the taxation sector. PPNS can now limit or terminate access to electronic systems used for criminal acts and request information from Electronic System Organizers to support investigations. This step allows for a faster response to cyber threats, such as data leaks or manipulation of the tax system. However, implementing this authority requires intensive training for PPNS to handle the complexity of cybercrime and ensure that digital evidence is managed according to legal procedures. In addition, harmonization between the latest UU ITE and other tax regulations is needed so that regulatory integration runs effectively without overlapping. With this approach, the latest UU ITE can be an important instrument in maintaining the integrity of the taxation system in the digital era.

At the international level, the OECD initiative to address Base Erosion and Profit Shifting (BEPS) is an important step in global tax harmonization. The BEPS Action Plan, especially Action 1, which focuses on the challenges of the digital economy, provides a framework to address cross-border tax avoidance. Indonesia, as a member of the G20, has committed to implementing BEPS recommendations, including strengthening regulations related to cross-border electronic transactions and taxation of the digital economy.

The Economic Theory of Crime proposed by Gary Becker (1968) provides an important perspective in understanding the motivation behind cybercrime in taxation. This theory states that individuals will commit crimes if the expected benefits exceed the costs or penalties that will be incurred.[32] In the context of digital taxation, this means that prevention efforts must focus not only on increasing penalties, but also on reducing the opportunities and increasing risks of being caught for criminals. The latest UU ITE has strengthened sanctions for various types of cybercrime, which is in line with the principles of this theory.

Facing the evolution of cybercrime in the digital tax system, a holistic approach is needed that involves strengthening regulations, improving technological capabilities, and educating taxpayers. The development of a more sophisticated cybersecurity system, increasing international cooperation in the exchange of tax information, and continuous training for tax officers in digital forensics are key. Harmonization of international tax regulations and consistent implementation of BEPS recommendations will help close the gap for cross-border tax evasion. With this comprehensive approach, supported by the latest UU ITE, the integrity of the tax system can be maintained, and potential state losses due to cybercrime can be minimized effectively, ensuring a fair and transparent tax system in the digital era.

Strategies and Challenges in Handling Tax Cybercrime

Strategies and challenges in addressing tax cybercrime have become a major focus for countries around the world. The United States has taken a proactive step by passing the Critical Infrastructure Cyber Incident Reporting Act in 2022. This law aims to improve information sharing between the private sector and the government to strengthen national cyber defences. In April 2024, the Cybersecurity and Infrastructure

[32]Doron Teichman. (2011). The Economics of Crime Control. Oxford Academi.

Security Agency (CISA) issued a rule requiring covered entities to report significant cyber incidents within 72 hours and ransom payments within 24 hours.[33] This move reflects the recognition of the importance of a rapid response to cyber threats in the tax context.

Australia has implemented digital tax forensics through technologies such as Universal Forensic Extraction software to support criminal investigations. The Australian Taxation Office (ATO) conducts legal investigations into tax evasion through warrants on taxpayers. Assets such as laptops or mobile devices are accessed in accordance with a court order that stipulates that material specifically relevant to the court order is held on the asset.[34] This approach demonstrates Australia's commitment to using advanced technology to combat digital tax crime.

In Indonesia, the Directorate General of Taxes (DGT) has implemented digital forensics as a tool in the tax law enforcement process. Through digital forensics, every digital tax crime can be revealed because it will leave traces in the form of digital files and documents. The digital tax forensics procedure in Indonesia is specifically regulated in SE-36/PJ/2017, which includes four main stages: data acquisition, data processing and analysis, reporting, and evidence storage.[35] However, the DGT's digital forensics procedure still tends to use semi-digital methods and has not fully adopted modern digital technology, which can be an obstacle if taxpayers remove and erase digital goods records.

The main challenge in implementing digital forensic technology in Indonesia lies in the complexity and dynamics of cybercrime, which continues to grow. The use of more sophisticated encryption technology and increasingly complex information-hiding strategies make the investigation process more complex.[36] This requires increased technological capabilities and expertise from law enforcement and security specialists to keep up with the development of technology used by cybercriminals.

The need for more comprehensive and effective regulations is becoming increasingly urgent. Law Number 1 of 2024 concerning the Second Amendment to the UU ITE provides a stronger legal basis for dealing with cybercrime, including in the context of taxation. The addition of Article 13A, which regulates Electronic Certification Provider services, such as electronic signatures and digital identities, provides a clearer legal framework to improve the security of electronic transactions in the taxation system.[37] However, further harmonization is still needed between the UU ITE and existing tax regulations to accommodate the complexity of cybercrime in taxation.[38]

The urgency of further research on the integration of big data analytics and artificial intelligence in the tax system is increasing. The use of AI in tax administration has proven to be effective in preventing tax irregularities and fraud, as well as

[33]Rajesh De, Adam S. Hickey, Stephen Lilley, Marcus A. Christian, Justin Herring, Amber C. Thomson, Aaron Futerman. (2024). Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act. Mayer I Brown

[34]Widya, A., & Suryani, Y. (2024). The Role of Tax Digital Forensic through the Utilization of Big Data Analytics in Indonesia. E-INVESTA: Jurnal Rumpun Ilmu Ekonomi dan Bisnis Islam, 1(1), 33-55.

[35]*Ibid*

[36]Monique, C., Yuliati, Y., & Sulistio, F. (2024). Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia's Criminal Procedure Law. Pena Justisia: Media Komunikasi dan Kajian Hukum, 23(2), 825-838.

[37]*Vide* Pasal 13 A Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

[38]Fahira, S. H., Daimah, D., & Mu'amar, I. (2024). Cryptocurrency Regulation in Indonesia: Regulation Review and Potential Risks from A Cyber Law Perspective. Indonesian Cyber Law Review, 1(1), 1-12.

improving the taxpayer experience. In Austria, the use of AI helped increase tax revenues by €185 million in 2023. The Competence Center for Forecasting Analytics of the Ministry of Finance used AI and machine learning algorithms to examine 34 million cases and selected 375,000 suspicious cases for in-depth examination. This shows the great potential of AI in increasing the efficiency and accuracy of tax crime detection.

The implementation of AI in tax systems also brings its own challenges, particularly in terms of data quality, privacy concerns, and the need for continuous model adaptation to evolving fraud tactics. Studies have shown that AI-based systems demonstrate higher accuracy in detecting complex fraud patterns compared to traditional rule-based approaches, with some implementations showing improvements of up to 85% in fraud detection rates.[39.40] However, challenges remain in terms of data quality, privacy concerns, and the need for continuous model adaptation to evolving fraud tactics.

International tax harmonization is key to addressing increasingly global tax cybercrime. The OECD initiative to address Base Erosion and Profit Shifting (BEPS) is an important step in global tax harmonization. The BEPS Action Plan, especially Action 1, which focuses on the challenges of the digital economy, provides a framework to address cross-border tax evasion.[41] Indonesia, as a member of the G20, has committed to implementing BEPS recommendations, including strengthening regulations related to cross-border electronic transactions and taxation of the digital economy.

A holistic approach involving strengthening regulations, improving technological capabilities, and educating taxpayers is becoming increasingly important. Developing more sophisticated cybersecurity systems, enhancing international cooperation in the exchange of tax information, and continuing training for tax officials in digital forensics are key to addressing these challenges. Harmonizing international tax regulations and consistently implementing BEPS recommendations will help close the gap for cross-border tax avoidance.

Finally, a comprehensive national strategy to combat tax crime is essential, not only to ensure that the country collects what it is supposed to but also to provide the foundation for a fair and transparent tax system. This strategy should include a process to identify key risks and involve collaboration with other relevant institutions and stakeholders.[42] With this comprehensive approach, the integrity of the tax system can be maintained, and potential state losses due to cybercrime can be effectively minimized, ensuring a fair and transparent tax system in the digital age.

CONCLUSIONS AND SUGGESTIONS

Cybercrime in taxation has developed into a serious threat, as seen from the case of the leak of 6 million NPWP data by hacker Bjorka in September 2024. Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas UU ITEhas strengthened the protection of online privacy, but harmonization with existing tax regulations is still

[39]PWC. (2020). Role of AI in transforming how tax authorities work. https://www.pwc.com/lv/en/about/services/IT-services/related-articles/Role-of-AI-in-transforming-how-tax-authorities-work.html. Diakses tanggal 01 Januari 2025

[40]Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., & Ishola, O. (2024). Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.

[41]OECD. (2024). Designing a National Strategy against Tax Crime Core Elements and Considerations. OECD Publishing, Paris, https://doi.org/10.1787/0e451c90-en.

[42]*Ibid*

needed. The use of digital forensics and artificial intelligence (AI) has proven effective in preventing tax fraud, as demonstrated by an increase in tax revenue of €185 million in Austria in 2023 thanks to the use of AI.

The Indonesian government needs to take concrete steps to strengthen the digital tax system. First, implementing a more sophisticated digital forensic system, such as the Universal Forensic Extraction software used in Australia. Second, integrating AI and big data analytics in tax administration systems to improve fraud detection, with the target of increasing the fraud detection rate by up to 85%. Third, increasing training for Civil Servant Investigators (PPNS) in handling tax cybercrime. Lastly, strengthen international cooperation in the exchange of tax information and the implementation of BEPS recommendations to address cross-border tax avoidance.

REFERENCES

Books by author:

Doron Teichman. (2011). The Economics of Crime Control. Oxford Academi.

James R. White. (2011). Taxes and Identity Theft Status of IRS Initiatives to Help Victimized Taxpayers. United States Government Accountability Office.

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). Metode penelitian hukum. CV. Gita Lentera.

Megumi Kashiwagi.(n.d). Problem of Identity Theft and Fraudulent Tax Refunds in the United States: Considering the Possible Developments Following a Future Consumption Tax Increase and Introduction of the Social Security and Tax Number System. The Canon Institute for Global Studies.

Syahril, M. A. F. (2023). Hukum Informasi dan Transaksi Elektronik.

Journal articles:

Ariyibi, K. O., Bello, O. F., Ekundayo, T. F., & Ishola, O. (2024). Leveraging Artificial Intelligence for enhanced tax fraud detection in modern fiscal systems.

Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., ... & Persi Paoli, G. (2020). The future of cybercrime in light of technology developments.

Fahira, S. H., Daimah, D., & Mu'amar, I. (2024). Cryptocurrency Regulation in Indonesia: Regulation Review and Potential Risks from A Cyber Law Perspective. Indonesian Cyber Law Review, 1(1), 1-12.

Karović, S., & Simović, M. (2022). Krivičnopravni I Viktimološki Aspekt Maloljetničke Delinkvencije–Izazovi, Dileme. Društvene Devijacije, 7(1).

Madani, L., Sofia, A., & Widarsono, A. (2024). The Influence of Cybersecurity Disclosure, Tax Risk, Reputation and Auditor Experience on Audit Quality. Jurnal Pendidikan Akuntansi & Keuangan, 12(2), 138-149.

Maris, A. W. (2024). Analisis Yuridis Tindak Pidana Perpajakan sebagai Salah Satu Modus Operandi Tindak Pidana Korupsi di Indonesia. Demokrasi: Jurnal Riset Ilmu Hukum, Sosial dan Politik, 1(3), 197-206.

Monique, C., Yuliati, Y., & Sulistio, F. (2024). Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia's Criminal Procedure Law. Pena Justisia: Media Komunikasi dan Kajian Hukum, 23(2), 825-838.

Nabila, L., & Setianingrum, R. B. (2024). Analisis Perlindungan Data Pribadi bagi Pengguna E-commerce Menurut Perspektif Hukum di Indonesia. Media of Law

and Sharia, 6(1), 1-17.
Rahayu, S. K. Keamanan Digital dalam Audit Pajak. Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance.
Rajesh De, Adam S. Hickey, Stephen Lilley, Marcus A. Christian, Justin Herring, Amber C. Thomson, Aaron Futerman. (2024). Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act. Mayer I Brown.
Rio Christiawan. (2023). Membaca Ulang Eksistensi Teori Pada Penelitian Normatif. https://www.hukumonline.com/berita/a/membaca-ulang-eksistensi-teori-pada-penelitian-normatif-lt64f99dc2f2924/. Diakses tanggal 31 Desember 2024.
Syahril, M. A. F., & Hasan, H. (2024). A Comparative Research on the Effectiveness of Progressive versus Proportional Tax Systems in Enhancing Social Justice. Administrative and Environmental Law Review, 5(2), 97-106.
Widya, A., & Suryani, Y. (2024). The Role of Tax Digital Forensic through the Utilization of Big Data Analytics in Indonesia. E-INVESTA: Jurnal Rumpun Ilmu Ekonomi dan Bisnis Islam, 1(1), 33-55.

World Wide Web:
Nadya Britton. (2024). Tax season is on its way and so is cybercrime: Cybersecurity considerations for tax firms. https://www.thomsonreuters.com/en-us/posts/tax-and-accounting/cybersecurity-considerations/
Nina Susilo, Mawar Kusuma Wulan. (2024). When the President's and His Family's and Ministers' Data is Leaked and Sold. https://www.kompas.id/baca/english/2024/09/23/en-ketika-data-presiden-keluarganya-dan-para-menteri-dijual
OECD. (2024). Designing a National Strategy against Tax Crime Core Elements and Considerations. OECD Publishing, Paris, https://doi.org/10.1787/0e451c90-en
PWC. (2020). Role of AI in transforming how tax authorities work. https://www.pwc.com/lv/en/about/services/IT-services/related-articles/Role-of-AI-in-transforming-how-tax-authorities-work.html
PWC. (2022). Cyber breach reporting to be required by law for better cyber defense.
USAFacts team. (2023). How many cyber-attacks occur in the US?. https://usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us/
Vassilis Kontoglis. (2024). Tax Season Brings Rise in Cyber Crime. https://www.aafcpa.com/2024/01/30/tax-season-brings-rise-in-cyber-crime/
Wibi Pangestu Pratama. (2024). Data Ditjen Pajak Diduga Bocor, Ada NPWP Jokowi, Gibran, Kaesang, hingga Sri Mulyani. https://ekonomi.bisnis.com/read/20240918/259/1800454/data-ditjen-pajak-diduga-bocor-ada-npwp-jokowi-gibran-kaesang-hingga-sri-mulyani.

Legislation:
Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.