Research Article

International Journal for Public Policy, Law and Development

Volume 2, Issue 2, Year 2025

Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data

Darina Shamatonova[1]

[1]Université catholique de Lyon, Lyon, France

Corresponding Author:
Darina Shamatonova
Université catholique de Lyon, Lyon, France
E-mail: d.shamatonova@gmail.com

Received: 17-03-2025, Manuscript No. JQR/IJPLD/27; **Editor Assigned:** 18-03-2025, Manuscript No. JQR/IJPLD/27; **Reviewed:** 02-04-2025, Manuscript No. JQR/IJPLD/27; **Published:** 30-04-2025

ABSTRACT:

This paper addresses the issue of contemporary regulation of data theft and critically evaluates the challenges of existing cybercrime offences based on the draft UN Convention on Cybercrime in comparison to the Russian Federation effective regulation. The draft United Nations Convention on Cybercrime is aimed at strengthening international cooperation for combating certain crimes committed by means of information and communication technology systems and for the sharing of evidence in electronic form of serious crimes. Recently, the United Nations Ad Hoc Committee, held in New York, reached an agreement on the draft convention and it will soon be submitted to the UN General Assembly for formal adoption.

KEYWORDS: Stealing data, Cybercrime, Unconvention, Cybersecurity, Data, Theft, Crimeasaservice

1. INTRODUCTION

On 8th of January 2024 Ukrainian hacker group "Kiborg" has put major Russia's Alfa-Bank's full client database into the public domain[1]. The hackers describe themselves as a "project of journalists and IT specialists united together in the fight against aggression in the information space". They leaked huge amounts of confidential banking and personal data (a database containing full names, dates of birth, telephone numbers and account details of 38 million customers) onto a publicly accessible website[2]. This example clearly shows how insecure data can be in the hands of cybercriminals, even when stored by professional companies with strong cybersecurity measures. And it raises the question of how to combat and prevent such excesses in the future, how to hold criminals accountable, especially extraterritorially.

I. Current prevalence of digital data theft offences

In December 2023 the studio behind the popular video game Spider-Man 2 was hacked and the details of the upcoming game, along with employee and company data, were stolen[3]. In November 2023 the British Library' customer data was leaked on the dark web[4]. In July 2022 Crypto.com, a world leading cryptocurrency exchange, was hacked and the personal data of over 700,000 users was stolen[5]. Up to the date number of cyberattacks for the purpose of stealing and compromising personal and corporate data increases in its quantity and scale. Data theft is the act of stealing computer-based information in digital form made usually for the purposes to compromise information or for its appropriation, or for further sale or dissemination. Because the data is incorporeal (as apart to the corporeal assets) and still remains with the owner, the stealing actually means getting access to the data.

CITE THIS ARTICLE: Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data. (2025). International Journal for Public Policy, Law and Development, 2(2), 1-5. https://ijpld.com/ijpld/article/view/27

International Journal for Public Policy, Law and Development

Volume 2, Issue 2, Year 2025

People experienced in breaking cybersecurity measures provide their services for payment (crime as a service), and can be located anywhere in the world: they do not need special tools, instruments or physical access to the premises, but just the internet connection and a computer. So, the computer crimes are widely spread across many countries and territories though most commonly such offences relate to specific categories of confidential information such as personal data, financial and credit cards data, contact details, trade secrets, intellectual property, information relating to national security, etc.[6] We should also take into account the enormous scale of cybercrimes, for instance, in 2020 in USA a lawsuit was filed against 4 Chinese nationals for hacking Equifax's (Georgia, US) computer network and stealing sensitive personally identifiable information of approximately 145 million US victims.[7] In 2016 a North Korean hacking group called Lazarus successfully stole millions of dollars by targeting the SWIFT global banking money transfer system. Lazarus has also stolen over 500 million dollars' worth of cryptocurrency.[8] During the MSP Theft Campaign,[9] Zhu, Zhang (from China) and their co-conspirators in the APT10 group successfully obtained unauthorized access to computers providing services to or belonging to companies located in at least 12 countries, including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, UAE, UK, US. APT10 group stole hundreds of gigabytes of sensitive data from victims' computer systems and continues to operate.

This extra-territorial aspect makes regulation of the crimes, the data theft in particular, much harder, since the source of information (target) may be located in one country and the criminal in another country. This makes criminal's conviction and arrest a highly difficult mission. Extraterritorial feature of data stealing creates a problem of deciding which legislation shall be applied to the offence, to the criminal, victim and how to tackle conflict of laws. It is important to mention that due to the remote character of work of cyber specialists they often move from place to place (digital nomadism) so that often citizenship differs from residency.

The jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes; lack of procedural powers; and lack of enforceable mutual assistance provisions with foreign states. The "I love you" virus creator is still unpunished because of the Philippines (his residence location) lacked appropriate computer crime statute at the time of the attack.[10] The crime may occur on the territory of one state, but the damage happens on the territory of another state or globally.

So, the existing cybercrime offences system is not effective in addressing the challenges raised by 'stealing' data. And therefore, the only way to resolve this issue is to use a unified global regulation (if this is at all achievable in the world having different legal systems, political regimes and tensions).

II. United Nations' Convention on Cybercrime as an international instrument combatting data theft

1. General Overview

An attempt at unification has been made by the United Nations in its project of Convention on Cybercrime,[11] but it is not in its final form and is still in the process of negotiation, with many comments from different participating countries[12] deriving from different legal systems and political tensions.[13] According to the Electronic Frontier Foundation "the treaty, if approved, may reshape criminal laws and bolster cross-border police surveillance powers to access and share user data, implicating the privacy and human rights of billions of people worldwide."[14]

The international legal framework under discussion is difficult to assess in terms of its effectiveness in combating data theft, as it is not yet in force and preliminary conclusions can only be drawn once it has entered into force and been put into practice. The proposed regulation of data theft is expressed in the draft Convention in Article 8 "Computer- related theft or fraud". The default version encourages contracting parties to adopt domestic legislation to make criminally punishable "committed intentionally and without right, the causing of a loss of property to another person <…> with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, an economic benefit or [computer data] [digital information] containing personal data, including information related to a person's bank account <…>".

The current and effective international legal instruments on the data theft are the Budapest Convention on Cybercrimes of 2001 and the European Union's Directive 2013/40/EU. The latter does not provide this exact type of cybercrime – data theft – and it has had to be interpreted trough a bunch of other offences, illegal access and, if appropriate, misuse of tools. The Budapest Convention in its Art. 8 "Computer-related fraud" touches upon loss of property by deletion of data or interference with the functioning of a computer system.[15] So, the great progress in

CITE THIS ARTICLE: Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data. (2025). International Journal for Public Policy, Law and Development, 2(2), 1-5. https://ijpld.com/ijpld/article/view/27

the new text of UN Convention is finally done in defining the most popular global computer crime, and it would finally receive a separate article thus creating a clear and unambiguous legal framework.

UN Convention draft defined all the elements required to effectively combat stealing data: definition of theft (even in the article's name), defining of computer data and (or) digital information as an object of "appropriation" and procurement of economic benefit, special mentioning of personal data and bank accounts as vulnerable kinds of information (actus reus) dishonest intent, intentional commitment and "without right" actions towards the person concerned (mens rea). A milestone here is that digital information, as an intangible, is recognized as a clear object that can be stolen. Participation and attempt in data theft are also criminalized (Art.19).

Nevertheless, the mere definition of a new offence does not itself guarantee success in combatting data theft, it requires complex of rules (and its seamless implementation into practice). Its effectiveness should also be supported by Article 16 on combatting of laundering of proceeds of crime, which criminalizes concealment of proceeds of crime, as it is understood that majority of cases of data theft are made out of lucrative interest. And more importantly, the effectiveness of a new article would depend also on jurisdiction clause (Article 22 of the draft UN Convention) and Chapter IV "Procedural measures and law enforcement".

2. Alternative proposals as to data theft complex regulation

Another interesting point could be found in additions, or alterations, that are proposed by group of countries of Russia, China, Iran, Venezuela, on which the EU and western countries protest. It is a proposal to criminalize provision of services (Art.10.ter of the UN Convention) and technical support or the creation of websites, communication networks with the intent to use it for the commission of stealing (or even provision of network services – in Art.10.quarter). Indeed, this proposal may be worth of consideration taking into account spread of darknet forums where hackers not only propose their help for committing crimes but also advertise and sell illegal results of such crimes. Forums and websites are the main communication channel for them to monetize results of illegal thefts.

For instance, RaidForums charged prices for offering access and downloading of stolen financial information, means of identification, and data from compromised databases. The interesting fact about it was that the main administrator of the forum was a 15-year-old child, who continued the forum's activity for 7 years. The problem was that it took years and significant law enforcement resources and cooperation to penetrate the dark web and shut down the platform.[16]

Moreover, in the light of the above example of the theft of 38 million bank customers' details, a ban on websites publishing, storing and making them publicly available would not be an excessive measure at all. As of the date of this paper the mentioned database is still publicly available at Kiborg's website[2] (it stays publicly available for 10 months in a row unprecedently breaching the privacy laws). There is no fair reason for not blocking this website and its content as one of the remedies. If the hosts or owners of the website would clearly understand that these actions are illegal under the threat of criminal charge, then dissemination of stolen data would not be so widespread. Sure, data might leak into the darknet or change storage media, but at least the information would not be so easily accessible.

Another proposal in the draft UN Convention is to create a separate criminal offence in relation to specifically personal data – Art.10.quinquies "Violation of personal data". This proposal concerns with the criminalizing sale, provision or otherwise making available of any material containing personal data to any other persons through the use of an information and communications technology system/device.

III. Regulation of stealing data in the Russian Federation

According to Art.5.1 of the Federal Law of the Russian Federation of July 27, 2006, No 149-FZ "On Information, Information Technologies and Information Protection" information can be the object of public, civil and other legal relationships and can be freely used by any person and transferred by one person to another person. Information is therefore a legally protected object and can be stolen (sold, transferred, copied, etc). The effective criminal laws of the Russian Federation do not have a specific offence[17] on theft of data and this offence is partly covered by illegal access breach, as in the Budapest Convention 2011. Illegal access (Art. 272 of the Criminal Code of the Russian Federation), misuse of tools (Art. 273), breach of exploitation rules of computers (Art. 274), critical infrastructure impact (Art. 274.1) and security breach (Art. 274.2) - this is the whole list of cybercrimes in Chapter 28 of the

CITE THIS ARTICLE: Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data. (2025). International Journal for Public Policy, Law and Development, 2(2), 1-5. https://ijpld.com/ijpld/article/view/27

Criminal Code. Besides, there is a specific article 159.6 in Chapter 21 dedicated to the crimes against property – "Fraud in the sphere of computer information". This is the theft of another person's property or the acquisition of the right to another person's property by entering, deleting, blocking, modifying of computer information, but this is not theft of information, it is a fraud carried out with the use of digital information or tools.

So criminal penalization under Russian rules would depend on the type of stolen information:

(1) if the information is of a personal character, i.e. personal data, the perpetrator would be held liable under the Article 137 of the Criminal Code "Violation of inviolability of private life": unlawful collection or dissemination of information about a person's private life or dissemination of such information in a public. Sanctions: fines and (or) imprisonment.

(2) if the information is of a business character, i.e. tax, banking, corporate or commercial secret, the perpetrator would be held liable under the Article 183 "Unlawful obtaining and disclosure of information constituting commercial, tax or banking secrets": collection of information by means of stealing of documents and by other illegal way (including with the use of digital means). Sanctions: fines and (or) imprisonment.

In addition, the offence would be qualified also under Article 272 "Illegal access" since the penetration was made by digital means. Illegal access means unlawful access to legally protected computer information, if this act resulted in e.g. copying of computer information. If the information is not of a personal or business nature, its theft would only be prosecuted as an illegal access offence.

Thus, according to the current wording of the Russian laws, there is no separate article for the theft of information which makes regulation of this type of crime highly ineffective. This being said in a context where one in four crimes is committed using digital technology[18] (according to the last known official statistical report of the RF Internal Affairs Ministry for the year 2022).

3. Conclusion

The Council of Europe's Convention on Cybercrime was created to address jurisdictional issue to assist in the successful prosecution of cyber criminals.[19] Only fostering international cooperation would prevent and combat cybercrimes more effectively at the national, regional and international levels. In addition, data theft laws should be written more clearly to clarify who should assume liability for stolen customer data or weak computer network defences,[20] on international and national levels, as of today, there is no separate offence of 'data theft' in either legal framework. On the whole, however, cybercrime law is an extremely limited mechanism for addressing online misconduct[21] and cannot alone prevent data theft; correct application of the laws and procedural mechanisms are required, as well as strong security measures undertaken by the owners and users of computer information. In any case, the draft Convention on Cybercrime represents an improvement by defining the crime of data theft, which could be a starting point in the hope of better protection in the future.

References

1. Novaya Gazeta Europe. (2024, January 8). Hackers publish personal data of 20 million Alfa-Bank customers. https://novayagazeta.eu/articles/2024/01/08/hackers-publish-personal-data-of-20-million-alfa-bank-customers-en-news
2. Kiborg. (2024, January 8). Злам Альфа-Банку два місяці потому. https://kiborg.news/2024/01/08/zlam-alfa-banku-dva-misyaczi-potomu/
3. BBC. (2023, December 19). Insomniac: Spider-Man 2 PlayStation studio victim of huge hack. BBC News. https://www.bbc.com/news/newsbeat-67754897
4. BBC. (2024). Entertainment & Arts: Cybercrime in media. https://www.bbc.com/news/entertainment-arts-67544504
5. TechRadar. (2022). Top data breaches and cyber attacks of 2022. https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022
6. Clough, J. (2011). Data theft? Cybercrime and the increasing criminalization of access to data. Criminal Law Forum, 22, 149.
7. Haris, A., & Zagaris, B. (2020). Cybercrime. International Enforcement Law Reporter, 36, 69.
8. Zagaris, B. (2022). Cybercrime. International Enforcement Law Reporter, 38, 161.

CITE THIS ARTICLE: Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data. (2025). International Journal for Public Policy, Law and Development, 2(2), 1-5. https://ijpld.com/ijpld/article/view/27

9. Zagaris, B. (2019). Cybercrime. International Enforcement Law Reporter, 35, 32.
10. Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal, 18, 426.
11. United Nations Office on Drugs and Crime (UNODC). (n.d.). Ad hoc committee on cybercrime – Sixth session. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main
12. United Nations Office on Drugs and Crime (UNODC). (2023, August 31). Draft treaty text. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_31.08.2023_PM.pdf
13. Foreign Policy. (2023, August 31). United Nations, Russia, and China: Cybercrime treaty. https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/
14. UNRIC. (n.d.). A UN treaty on cybercrime en route. https://unric.org/en/a-un-treaty-on-cybercrime-en-route/
15. Council of Europe. (n.d.). Convention on Cybercrime. https://rm.coe.int/1680081561
16. Zagaris, B. (2022). Cybercrime. International Enforcement Law Reporter, 38, 161. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_31.08.2023_PM.pdf
17. ZakonRF. (n.d.). Codes and laws. https://www.zakonrf.info/uk/?ysclid=lr7t7h0byt332707849
18. Ministry of Internal Affairs of the Russian Federation (MVD RF). (2023, January 20). Reports. https://xn--b1aew.xn--p1ai/reports/item/35396677/?year=2023&month=1&day=20
19. Weber, A. M. (2003). The Council of Europe's Convention on Cybercrime. Berkeley Technology Law Journal, 18, 425.
20. Ablon, L., & Libicki, M. (2015). Hacker's bazaar: The markets for cybercrime tools and stolen data. Defense Counsel Journal, 82, 151.
21. Mayer, J. (2016). Cybercrime litigation. University of Pennsylvania Law Review, 164, 1506.

CITE THIS ARTICLE: Are The Existing Cybercrime Offences Effective in Addressing the Challenges Raised By Stealing Data. (2025). International Journal for Public Policy, Law and Development, 2(2), 1-5. https://ijpld.com/ijpld/article/view/27