GIS Odyssey Journal

2023 • Volume 3 • Number 2

https://doi.org/10.57599/gisoj.2023.3.2.37

Agnieszka Gryszczyńska[1]

CRIMINAL LIABILITY FOR CLI SPOOFING

Abstract: Spoofing involves masking the identity of a person, group or organisation, by manipulating addresses, identifiers or other data used to identify a user or system. This can range from falsifying IP addresses, phone numbers and email addresses to generating persuasive, fake signals capable of disrupting the reception of legitimate GPS signals by receivers.

The article aims to analyse the criminal liability of spoofing attacks, with a focus on CLI spoofing. Additionally, the article will identify the most common methods used by perpetrators of spoofing attacks. This will be followed by an examination of the statutory measures implemented in Poland to mitigate the effects of spoofing attacks, which are considered as reasons for criminal responsibility.

The article confirms the research hypothesis that effective reduction of CLI spoofing requires not only legislation that introduces criminal liability for spoofing, but also appropriate legal regulations that impose certain obligations on telecommunications entrepreneurs, efficient international cooperation, and comprehensive education in the fields of cybersecurity and cyber hygiene.

Keywords: spoofing, cybercrime, smishing, abuse of electronic communication, hacking, cybersecurity

Received: 13 November 2023; accepted: 16 December 2023

[1] Cardinal Stefan Wyszyński University, Faculty of Law and Administration, Department of Informatics Law, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0003-3004-5253, email: a.gryszczyńska@uksw.edu.pl

Introduction

Electronic communication is used by several billion users. Global growth is being observed in the number of Internet users - in July 2023 they accounted for about 64.5% of the population. Unique mobile subscribers around the world accounted for an estimated 5.56 billion, equating to 69.1 % of the global population. Mobile phone adoption increased by 2.7 % over the past year, thanks to almost 150 million new users (DataReportal, 2023 a). The time that Internet users spend online varies meaningfully by geography and demography. In Poland, the average time spent online by Internet users aged 16 to 64 is 6 hours and 42 minutes, compared to a global average of 6 hours 37 minutes (DataReportal, 2023 b).

The proliferation of electronic communication services and the corresponding rise in online activity unfortunately provides an opportunity for criminal abuse. Incidents can vary in complexity, ranging from those that exploit very simple social engineering techniques to more sophisticated attacks that combine social engineering with the exploitation of vulnerabilities, loopholes, manipulation of computer systems and the use of disruptive technologies. The goals of perpetrators responsible for the abuse of electronic communications vary, however the primary goal is to achieve financial gain by acting to the detriment of end-users or companies providing interpersonal communication services.

One of the techniques used by offenders is spoofing. Spoofing can range from faking IP addresses, phone numbers, email addresses to generating false signals that are strong enough to interfere with receivers' reception of real GPS signals.

IP and email spoofing are prevalent among cybercriminals. IP spoofing is used to conceal the attacker's IP address, while email spoofing is often used to enhance the effectiveness of an attack rather than to conceal the attacker's email address. In recent years, in Poland, attacks where the perpetrators spoofed telephone numbers have been particularly troublesome. The significant number of attacks targeting politicians' personal information has prompted a wider discussion on how to counter CLI spoofing and how to investigate perpetrators using this technique.

The purpose of this article is to analyse criminal liability for attacks using spoofing. In addition, regulations introduced in Poland in 2023 by the Act on Combating Abuse in Electronic Communications (ACAEC), designed to limit spoofing, and in particular CLI spoofing, were discussed. The broader approach involving consideration of administrative law provisions is further aimed at verifying the effectiveness of this regulation in reducing CLI spoofing attacks and protecting victims.

The article verifies the research hypothesis, according to which not only legislation introducing criminal liability for spoofing, but more broadly appropriate legal regulations imposing certain obligations on telecommunications operators, efficient international cooperation, as well as comprehensive education in the field of cybersecurity and cyber hygiene are necessary to effectively reduce CLI spoofing.

Material and methods

The article applies primarily the dogmatic method, as the analysis of criminal liability for CLI spoofing was based both on selected normative acts and the literature on the subject. Complementarily, a comparative legal method was applied. The basis for the analysis was the Polish Act on Combating Abuse in Electronic Communications (ACAEC, 2023) and the Polish Criminal Code (PCC, 1997) and the solutions introduced in them related to differentiated liability for both spoofing and technical maintenance of infrastructure and services enabling such attacks.

State of a problem: the concept of spoofing

Activities in cyberspace allow perpetrators to maintain a high level of anonymity. Criminals attempting to conceal their own identity often use fictitiously created identities or assumed identities to do so. The problem of impersonation is complex and multidimensional (Gryszczyńska, 2020). Spoofing can be defined as the act of concealing the identity of a person, group or organisation by manipulating addresses, identifiers or other data, that can be used to identify a user or system. It is a tactic that involves hiding or disguising one's true identity, as well as manipulating data, changing attributes, or using certain tools to hide the identity of the originator. Additionally, spoofing aims not only at hiding the identity of the source but also at mimicking a trusted and legitimate source. The objective of spoofing is to deceive the target into thinking they are interacting with a trustworthy entity when this is not true. For spoofing to succeed, the user's trust is crucial. Spoofers exploit this trust to gain unauthorised access or deceive the recipient by posing as a trusted authority. By masquerading as a reliable source, spoofers can bypass security measures, enabling malicious content or activities to proceed without obstruction. Successful spoofing is characterised by its difficulty in being detected. Messages that seem to originate from a trustworthy source generally do not raise red flags, leading to difficulty for both systems and users in differentiating between legitimate and spoofed communications. It is important to note that spoofing is not a standalone crime, but rather a component of a multifaceted criminal act that aims to facilitate the perpetrator in achieving a specific objective (e.g. obtaining unauthorised information, financial gain, or causing harm).

The most common types of spoofing include: IP spoofing (source address manipulation), email spoofing (forgery of message headers), CLI Spoofing (Calling Line Identification Spoofing), text Spoofing (sending SMS or text messages from a forged sender, commonly used in smishing attacks), website spoofing, DNS Cache Poisoning (DNS Spoofing), Wi-Fi spoofing (impersonating access points), MAC Spoofing, ARP Spoofing (poisoning the ARP table), GPS spoofing (confusing navigation systems), biometric spoofing (deceiving recognition systems), SSL/TLS spoofing (forgery of certificates).

The use of the COVID-19 pandemic and social engineering based on it for massive cyber attacks, as well as swatting, which consists of sending information about planting explosives, as well as impersonating politicians' phone numbers to make criminal

threats against other people, triggered legislative action in Poland. As a result, on 28 July 2023, the Act on Combating Abuse in Electronic Communications (ACAEC, 2023) was adopted, which includes new obligations for telecommunications providers to combat abuse in electronic communications, as well as administrative (financial) and criminal sanctions.

The ACAEC broadly defines the misuse of electronic communications as the provision or use of a telecommunications service or the use of telecommunications devices contrary to their intended purpose or contrary to the law, the purpose or effect of which is to cause damage to a telecommunications operator or end-user or to obtain an undue advantage for the misuser of electronic communications, another natural person, legal person or unincorporated entity. Abuses of electronic communications under Article 3 of the ACAEC include, inter alia, the generation of artificial traffic, smishing, CLI spoofing and unauthorised modification of address information. A broad definition of spoofing among the abuses identified in Article 3 of the ACAEC would include both smishing, CLI spoofing and unauthorised modification of address information, i.e. the unlawful modification of address information that makes it impossible or significantly more difficult for authorised entities or telecommunications operators involved in the transmission of a communication to determine the address information of the user sending the communication. The definition of a communication in Polish law is very broad, encompassing any information exchanged or transmitted between specific users via publicly available telecommunications services (Article 2(17) Telecommunications Law, 2004). The definition of address information used by the Polish legislator is also very broad and includes both a telephone number and any other identifier of the user sending the message (Article 2(3) ACAEC). The identifier may therefore be a subscriber identification character, including an electronic address, a name, a code, a radio station identification character or an IP address.

It will therefore be an abuse of electronic communications to modify the address information of short text messages (including the so-called headers), multimedia MMS messages, as well as the address information of a voice call. It will not be an infringement to change only the IP address of the user sending the communication, as this is the basis for services such as VPN or PROXY.

Calling Line Identification Spoofing

Calling Line Identification spoofing (CLI spoofing) involves telephone calls being made using a false caller identifier (known as caller ID). Caller ID allows the caller's user number to be displayed on the recipient's telephone so that the recipient can decide whether to answer the call. This number is transmitted between operators without mechanisms to authenticate this information (i3Forum, 2020). A user of services that allow the impersonation of an MSISDN number, using the infrastructure of operators that violate the integrity of the network, can enter any telephone number to be displayed on the screen of the recipient of the call. The risk of impersonation of the originating number has not been taken into account in the design of telecommunications

networks, and the communication itself and the transfer of call bundles between operators is based on trust. Therefore, if the call originator pretends to be a different MSISDN number, the telecommunications network operators do not verify this information and the exchanges rely on the messages sent by the other exchanges. The services that enable call originator impersonation are readily available on the Internet and inexpensive, so the perpetrator does not need to have specific knowledge of how the telecommunications network works. For this reason, it is very easy for fraudsters to impersonate a specific number using Internet VoIP gateways. Examples of such impersonated voice calls include: calls originating from abroad where the address information indicates the number of a user in the country, voice calls impersonating an emergency number (e.g. 112), voice calls impersonating a number that does not comply with the national numbering plan.

The Polish legislator, when introducing the catalogue of telecommunications abuses in the ACAEC defined CLI spoofing as the unauthorised use or exploitation by a user or a telecommunications operator, making a voice call, of address information indicating a natural person, a legal person or an unincorporated organisational unit other than that user or telecommunications operator, legal person or unincorporated organisational unit other than that user or telecommunications undertaking, in order to impersonate another entity, in particular to cause fear or anxiety or to induce the recipient of the call to perform a specific act, in particular to disclose personal data, damage property or install software (Art. 3(1)(3) ACAEC). It should be noted, however, that the terminological scope of CLI spoofing as an abuse of electronic communications is broader than the scope of the offence under Article 31 ACAEC, which consists in the use of address information indicating another entity when making a voice call.

Attack scenarios that exploit CLI spoofing

As indicated in the literature, antispoofing has not been a major design consideration in the development of not only telecommunications networks and protocols, but also civil GPS and WAAS signal architectures. However, rapid progress in computing power has made it much more possible to create advanced "all software" spoofer systems. The widespread use of electronic communication and GPS technology in various applications has made it more appealing to carry out attacks, mainly in pursuit of financial gain (Scott, 2003). This trend is on the rise.

Spoofing, including CLI spoofing, is a global phenomenon and has been used in various criminal scenarios for many years. In particular, media reports of attacks in the USA are described and referred to as swatting, a crime that has evolved from a dangerous prank to a cybercrime that can be ordered as a service. Swatting is where someone makes a hoax emergency call to law enforcement in order to get armed police (hence the SWAT reference) to target a particular address. While the attacks vary in nature, it is significant that swatting also occurs in the Swatting-as-a-Service model. Using the anonymity provided by electronic communications, CLI spoofing and voices generated by artificial intelligence (AI), individuals or groups of individuals offer

swatting services for small fees to cause the evacuation of public facilities (Arntz, 2023). CLI spoofing is also used in fraudulent activities, which are becoming increasingly sophisticated and difficult to detect. It usually originates offshore, readily adapts to disruption measures and ruthlessly exploits new opportunities and vulnerabilities (C661:2022).

CLI spoofing in 2022 and 2023 in Poland was most commonly observed in scenarios where the perpetrator pretended to be a bank customer service call centre employee. The phone number displayed to the victim was that of the bank's call centre. Victims were most often informed that an attempt to allegedly break into a bank account had been detected and asked to install a remote desktop application that would give the perpetrators access to the victim's device. In scenarios where a bank call centre number has been impersonated, the perpetrators' aim is most often to phish for personal data, e-banking passwords, to induce a transfer to a specified bank account, to induce the installation of malware or other software that allows the perpetrator to access the victim's device.

For similar purposes and scenarios, the perpetrators impersonate the telephone number of a police unit (including, but not limited to, the telephone numbers of the Central Bureau for Combating Cybercrime), informing the victim of an alleged intrusion into their bank account and the need to transfer funds to another bank account. The perpetrators impersonate the telephone numbers of bank call centres or police units in order to increase the credibility of the socio-technical scenario and thus the effectiveness of the attack, the primary objective of which is to obtain the funds deposited in the victim's bank account.

CLI spoofing is also used to make criminal threats, harassment or to report a non-existent threat (e.g. planting explosives). A significant number of such incidents were reported in Poland in late 2021 and early 2022. The perpetrators impersonated the phone numbers of public figures, politicians, journalists and cybersecurity experts. In most cases, tools that convert text into synthetic speech (voice synthesizers) were used and a pre-recorded message was played. Given the modus operandi of the perpetrators, it should be noted that in this scenario the aim was to trigger action by law enforcement agencies (e.g. police) and services necessary to ensure safety and health protection (fire brigade, ambulance). The vast majority of these attacks also aimed to harm the person whose data was used, both by making them feel ridiculed or less credible, and by targeting them for law enforcement action. Persons whose telephone numbers have been impersonated and whose data have been used should therefore in principle be considered as victims of identity theft (i.e. the offence defined in Article 190a § 2 PCC). Unfortunately, in some cases victims of identity theft have been treated as perpetrators of criminal threats (i.e. an offence under Article 190a § 1 PCC) or swatting (Article 224a PCC).

Misdirected pre-trial investigations in CLI spoofing cases can be avoided by a thorough analysis of the connection lists for the MSISDN to which the call was made and the MSISDN that allegedly initiated the call (the impersonated number). The purpose of comparing the incoming and outgoing calls for both numbers is to check that

the call under investigation is included in the call lists of both MSISDNs and that the data relating to this call is the same on both call lists (as regards the start and end time of the call). Spoofing may also be indicated by discrepancies in the time at which the call should have been established, the termination of the call or the duration of the call, the absence of the IMEI number of the device or BTS data in the call list.

Identifying the person responsible for a particular attack and the infrastructure provider is not easy because the perpetrators of individual attacks use foreign telecommunications infrastructure. In addition, the connection is repeatedly routed between different operators. In order to determine where the call originated, law enforcement authorities should, after obtaining data from the call list indicating spoofing, request the telecommunications operator to provide the call path, i.e. data on the operator from whose network the call was routed. Once this information has been obtained, a similar request should be made to the next operator. Since in all the cases analysed for the purpose of this article, calls to the Polish network were routed from foreign operators, it was necessary to use the instruments of international legal cooperation in order to establish the path of the call. Due to the critically short period of time during which data was stored to allow tracing a connection, even the immediate preservation of data in accordance with Article 29 of the Convention on Cybercrime (2001) did not make it possible to determine the originator of the connection.

The effectiveness of the attacks in which CLI spoofing was used indicates the need for widespread educational efforts to raise awareness of the risks and cyber hygiene. In cases of CLI spoofing, the victim would not have been harmed if he or she had ended the call and called back the number that the perpetrators were impersonating.

The offence of spoofing in Poland

The Act on Combating Abuse in Electronic Communications contains four criminal provisions. These introduce criminal liability for the generation of artificial traffic (Article 29), smishing (Article 30), CLI spoofing (Article 31) and modification of address information (Article 32).

According to Art. 31 of the ACAEC states that anyone who, with the aim of obtaining a financial or personal advantage or causing damage to another person, uses, without being entitled to do so, address information identifying another natural person, legal person or organisational unit without legal personality, when making a voice call, in order to impersonate another entity, in order to induce the recipient of such a call to disclose personal data, to dispose unfavourably of property or to install software, to disclose computer passwords, access codes or other data allowing unauthorised access to information stored in a computer system, data communication system or data communication network. In its basic type, this offence is punishable by imprisonment from 3 months to 5 years; in the case of lesser gravity, the perpetrator is subject to a fine, restriction of liberty or imprisonment for up to one year. Only if the offence is committed against a person close to the perpetrator is the victim prosecuted.

This is a intentional offence. Since the perpetrator must act with the aim of obtaining financial gain, personal advantage or causing harm to another person, and then with the aim of inducing the recipient of the call to disclose personal data, dispose of property or install software, disclose computer passwords, access codes or other data that allows unauthorised access to information, from a subjective point of view – direct intent is required.

The use by the offender of address information indicating another entity in a voice call is intended to impersonate another entity in order to induce the recipient of the call to act in a particular way. However, it is not necessary to achieve the objective in order to fulfil the elements of the offence. Even if the recipient of the call does not transmit data or install malicious software, the mere impersonation of another entity makes the offence under Article 31 ACAEC an offence and not merely an attempt. The offence is therefore of a formal nature.

It should be stressed that Article 31 only defines criminal liability for the use of address information impersonating another entity when making a voice call. Pretending to be another entity when sending a text message (SMS), a multimedia message (MMS) or a message via other interpersonal communication services is punishable under Article 30 of the ACAEC.

The most general provision relating to the modification of address information is Article 32 of the ACAEC, which covers the unlawful modification of address information that prevents or significantly impedes the determination of the address information of the user sending the communication by the authorised entities or telecommunications undertakings involved in the delivery of the communication, for the purpose of obtaining a pecuniary advantage, personal benefit or causing harm to another person. For the purposes of fulfilling the elements of Article 32 ACAEC, it is also not necessary to analyse whether the impersonator's purpose was to induce the recipient of the communication to disclose personal data, to dispose of property, to install software, to disclose computer passwords, access codes or other data allowing unauthorised access to information. It is sufficient to establish that the primary objective of the perpetrator is to obtain financial gain or personal advantage or to cause harm to another person, without examining his or her indirect objective. Article 31 ACAEC is therefore *lex specialis* to Article 32 ACAEC.

According to the general conflict rule that the more specific law should be applied before the more general law (*lex specialis derogat legi generali*), Article 31 of the ACAEC should apply to scenarios of attacks primarily aimed at monetisation, i.e. the impersonation of banks or police officers described above in order to defraud e-banking data, induce a transfer or install software. For scenarios where the perpetrators impersonate another person's telephone number in order to make criminal threats or to inform about a non-existent threat, Article 32 of the ACAEC will apply.

In principle, the criminal provisions of the ACAEC will not be the only basis for the perpetrator's liability, as changing address information is not an end in itself, but a means to another end. When determining the liability of an offender using CLI spoofing and directing criminal threats, criminal liability for identity theft (Article 190a § 2 PCC)

and directing criminal threats (Article 190 § 1 PCC) should also be taken into account. In swatting cases, criminal liability for identity theft (Art. 190a § 2 PCC) and inducing an institution to act by reporting a non-existent threat (Art. 224a PCC) should be taken into account. In cases involving monetisation, depending on the scenario, criminal liability for fraud (Art. 286 § 1 PCC), computer fraud (Art. 287 § 1 PCC), break-in (Art. 279 § 1 PCC) and hacking (Art. 267 § 1 PCC).

If the perpetrator's actions are considered to constitute a single offence which fulfils the elements set out in two or more provisions of the criminal law, the court will convict the perpetrator of a single offence on the basis of all the concurrent provisions. The court will punish the offender on the basis of the provision that provides for the most severe punishment. In swatting cases – the most severe punishment is provided by Article 224 a PCC (8 or 12 years imprisonment), if the perpetrator fulfils the elements of identity theft - Article 190 a § 2 PCC (8 years), if the remaining provision in concurrence is Article 286 § 1 PCC (8 years) or Article 279 § 1 PCC (10 years), these articles will be the basis for the punishment, as the upper limit of criminal liability for acts under Articles 31 and 32 ACAEC is 5 years imprisonment.

Results and discussion: effectiveness of criminal law regulation vs. other measures

In the current network environment, there are an increasing number of untrustworthy devices (including the private automatic branch exchange, call centre and VoIP access system) that interconnect to a public land mobile network/public switched telephone network. As a result, a large number of phone numbers are leased to anonymous call providers who help fuel phone spam. Calls with spoofed numbers come from all over the world and account for a significant and growing proportion of nuisance calls.

The perpetrators – both those responsible for providing the infrastructure necessary for spoofing and those who use this infrastructure for impersonation – are extremely difficult to identify due to the anonymisation methods they use. The low detection rate of CLI spoofing perpetrators means that criminal provisions will not be effective. Diverse measures are needed to reduce CLI spoofing and its negative effects.

Caller ID spoofing, although a common threat, can be effectively minimized with modern technologies and standards. Two key solutions are STIR/SHAKEN and robocall blocking. While these technologies are available, their effectiveness depends on their proper implementation. All network operators must update their systems to support STIR/SHAKEN protocols, and users must take advantage of the robocall blocking option, if available. Each network must confirm the authenticity of a caller's number before forwarding the call to the next network. This means that all operators around the world must update their systems to support these protocols. For obvious reasons, this is a postulate that is impossible to implement on a global scale. However, these solutions are being introduced locally (Telephone Robocall Abuse, 2020). In addition, they are accompanied by the imposition of various obligations on telecommunications

entrepreneurs (US TRACED Act, 2019). Those who do not fulfil these obligations may be subject to legal liability (U.S. Dept. of Justice, 2020).

In addition to the criminal liability discussed above, the Polish law also provides for a number of obligations imposed on telecommunications operators to take proportionate (and risk-based) measures to prevent and combat the misuse of electronic communications. One such measure is the monitoring of telecommunications services to detect cases of CLI spoofing. Article 16 of the ACAEC imposes an obligation on a telecommunications undertaking to either block a voice call or to conceal the identification of the calling number to the end-user when CLI spoofing occurs. Voice call blocking should be used when the likelihood of CLI spoofing is very high or high. In other cases, the telecommunications undertaking should conceal the caller identification from the end user. Hiding the caller identification means in practice that the recipient is told that an unknown number is calling, rather than being told, for example, that a close friend whose number is in the contact list is calling.

To effectively combat CLI spoofing, a telecommunications operator must also be able to monitor traffic on the telecommunications network to detect suspicious voice calls. Measures are also needed to enable the exchange of information about such calls between operators – traffic on the telecommunications network is often routed through the telecommunications networks of different operators. Finally, measures are needed to deal with suspicious calls – either to block such a call or to conceal the identification of the calling number from the end user. According to Article 19 of the ACAEC, the telecommunications undertaking shall apply organisational and technical measures to monitor, detect and exchange information on CLI spoofing and either block the voice call or conceal the caller identification to the end user. A provider of publicly available telecommunications services who provides telecommunications services to at least 50,000 subscribers and who is also an operator may enter into an agreement with the President of the Office for Electronic Communications in which it specifies the detailed organisational and technical measures it will apply in fulfilling the obligations referred to in Article 16. The drafting of this provision was based on Recommendation M.3362 of the International Telecommunications Union (M.3362, 2020). By signing and correctly implementing this agreement, operators fulfil their obligation to take appropriate organisational and technical measures to prevent CLI spoofing. The ACAEC also introduces an exemption from liability for non-performance or improper performance of the telecommunications service for those operators that correctly implement the agreement. The exemption from liability for correct implementation of the agreement will provide a strong incentive to join the agreement. With this solution, the largest telecommunications operators, with the support and supervision of the Office for Electronic Communications, will be able to develop the best organisational and technical solutions to combat abuse in electronic communications. For smaller telecommunications operators that may not be able to fulfil the obligations set out in the agreement, the President of the Office for Electronic Communications will issue recommendations specifying organisational and technical measures to implement the obligations related to combating CLI spoofing. The correct implementation of the

recommendations of the President of the Office for Electronic Communications will exclude the liability of these operators for the non-performance or improper performance of telecommunications services resulting from the introduction of these measures.

In addition, taking into account the fact that criminals very often impersonate call centre numbers of various entities that are only used to receive calls and not to call customers, a mechanism has been introduced to prevent impersonation of these numbers. Pursuant to Article 17 of the ACAEC, the President of the Office for Electronic Communications shall maintain, by means of an ICT system, an unclassified list of numbers used only for receiving voice calls and shall make this list available in the Public Information Bulletin on his authority's website. Banks and public financial institutions, among others, may request to be included in the list. It is the responsibility of the telecommunications company providing the voice call service to block incoming calls to its network using a number included in the list.

Apart from criminal liability, the ACAEC contains provisions on administrative fines. Not only a telecommunications operator who commits an abuse of electronic communications, such as the generation of artificial traffic, smishing, CLI spoofing, unauthorised change of address information, but also a telecommunications operator who fails to comply with the obligations imposed by Articles 16 and 17 of the ACAEC may be fined. It should be noted, however, that if an act constituting an abuse of electronic communications also exhausts the elements of a criminal offence, only the provisions on criminal liability apply to a telecommunications operator that is a natural person.

It should also be noted that an administrative fine will be introduced for the four abuses of electronic communications mentioned above. For the remaining abuses, a specific entity may be held criminally liable and subject to general civil liability rules.

Irrespective of the fine imposed on a telecommunications undertaking, the President of the Office for Electronic Communications may, by decision, impose a fine of up to 300% of the monthly earnings of the management of a telecommunications operator.

Conclusions

Countering and combating electronic communication abuse requires a variety of legal, organizational, and technical measures due to its multifaceted and intricate nature.

Some opinions on the draft ACAEC, however, pointed out that phenomena such as smishing, CLI spoofing or unauthorised change of address information do not require such extensive criminalisation and that administrative or misdemeanour penalties would be sufficient for these behaviours (Supreme Court of the Republic of Poland, 2023). However, given the specific nature of the actions of the infringers, it should be considered that such an adoption of the scope of liability, taking into account the limited legal means to establish the identity of those responsible for providing the infrastructure enabling CLI spoofing and impersonation of other subscribers, would

make administrative and misdemeanour liability only illusory. It is only through criminal law that specific information can be gathered quickly to identify the person or entity responsible. Especially as the cases in which CLI spoofing is used are of a cross-border nature.

Irrespective of criminal liability, there is a need for provisions that impose certain obligations on telecommunications undertakings in relation to the prevention of telecommunications abuse against certain persons who are perpetrators of the offences set out in the ACAEC or the PCC. Administrative fines should be provided for violations by the telecommunications providers themselves or for not implementing the obligations related to the protection of users.

Entrepreneurs will only make the financial effort to implement certain technical measures if the supervisory authority can impose a financial penalty on the entrepreneur (and at the same time the management of the company).

At the same time, the effects of CLI spoofing can be mitigated by widespread and mass cybersecurity education. The formation of habits related to the verification of information and the verification of the identity of the caller are the fundamentals of cyber hygiene.

The article confirms the research hypothesis that effective reduction of CLI spoofing requires not only legislation that introduces criminal liability for spoofing, but also appropriate legal regulations that impose certain obligations on telecommunications entrepreneurs, efficient international cooperation, and comprehensive education in the field of cybersecurity.

References

ACAEC (2023). Act of 28 July 2023 on Combating Abuse in Electronic Communications. Journal of Laws 2023, item 170.

Arntz P. (2023). Swatting-as-a-Service is a growing and complicated problem to solve. https://www.malwarebytes.com/blog/news/2023/04/swatting-as-a-service-is-a-growing-and-complicated-problem-to-solve [access: 25.11.2023].

C661:2022. Reducing Scam Calls and Scam SMS. Industry Code. Communications Alliance LTD. https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf [access: 25.11.2023].

DataReportal (2023 a). Digital 2023 October Global Statshot Report. https://datareportal.com/reports/digital-2023-july-global-statshot [access: 17.11.2023].

DataReportal (2023 b). Digital 2023 Global Overview Report. https://datareportal.com/reports/digital-2023-global-overview-report [access: 17.11.2023].

Gryszczyńska A. (2020). Identity theft in cybercrime cases. In: Yearbook of Maritime Security, Teleinformation Crime 2019, J. Kosiński, G. Krasnodębski (ed.). Gdynia, pp. 207–227.

i3Forum (2020). International Interconnection Forum for Services over IP (i3 FORUM). Technical Report Calling Line Identification (CLI) spoofing (Release 1.0) October. https://i3forum.org/blog/2020/11/04/i3forum-calling-line-identification-cli-spoofing-report/[access: 17.11.2023].

M.3362. 2020. Recommendation M.3362 (06/20). Requirements for telecommunication anti-fraud management in the telecommunication management network. International Telecommunication Union. https://www.itu.int/rec/T-REC-M.3362-202006-I/en [access: 25.11.2023].

PCC (1997). Criminal Code of June 6, 1997. Journal of Laws of 2022, item 1138, as amended.

Scott L. (2003). Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems, Conference Paper. ION GPS/GNSS 2003. Portland, OR.

Supreme Court of the Republic of Poland (2023). Opinion on the government draft law on combating abuse of electronic communications. Sejm print no. 3069. Supreme Court of the Republic of Poland.

Telecommunications Law (2004). Telecommunications Law of 16 July 2004. Journal of Laws 2022 items 1648, 1933 and 2581 and 2023 items 1394 and 1703.

Telephone Robocall Abuse (2020). Telephone Robocall Abuse Criminal Enforcement and Deterrence Act 2020. Report to Congress. U.S. Department of Justice. https://www.justice.gov/opa/press-release/file/1331576/download [access: 25.11.2023].

The Convention on Cybercrime of the Council of Europe (CETS No. 185) (2001). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [access: 25.11.2023].

U.S. Dept. of Justice (2020). The Department of Justice Files Actions to Stop Telecom Carriers Who Facilitated Hundreds of Millions of Fraudulent Robocalls to American Consumers. https://www.justice.gov/opa/pr/department-justice-files-actions-stop-telecom-carriers-who-facilitated-hundreds-millions [access: 25.11.2023].

US TRACED Act (2019). Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (Public Law 116–105). https://www.govinfo.gov/content/pkg/PLAW-116publ105/pdf/PLAW-116publ105.pdf [access: 25.11.2023].