Articles Studia Iuridica Lublinensia vol. 34, 2, 2025
DOI: 10.17951/sil.2025.34.2.321-341

Maciej Siwicki
Nicolaus Copernicus University in Toruń, Poland
ORCID: 0000-0002-3120-0211
msiwicki@umk.pl

Comparative Legal Frameworks for Protecting Elderly People from Cyberfraud

Analiza porównawcza przepisów prawnych dotyczących ochrony osób starszych przed oszustwami internetowymi

ABSTRACT

Recent years have seen a dramatic increase in cybercrime targeting seniors. In countries like Poland, specific scam methods such as the "grandson" or "policeman" trick and phishing attacks have become prevalent, often resulting in the loss of life savings. Despite the growing scale of the problem, criminology faces challenges in accurately measuring the extent of internet fraud. The internet's reach and anonymity facilitate these crimes, making detection and prevention more difficult than with traditional methods. This raises critical questions about the adequacy of current legal protections for the elderly and whether criminal law should address the exploitation of their gullibility or ignorance. By examining legal definitions, perpetrators' modus operandi, and comparative international solutions, the study aims to assess whether existing frameworks sufficiently safeguard seniors and to explore the potential for harmonized cross-border legal measures to better protect this increasingly targeted demographic.

Keywords: elderly people; internet fraud; comparative law; cybercrime

INTRODUCTION

In recent years, elderly people have increasingly become victims of online theft, burglary and fraud. For example, according to estimates presented by the FBI, senior citizens in the USA lost more than $3.4 billion to financial scams in 2023

CORRESPONDENCE ADDRESS: Maciej Siwicki, PhD, Dr. Habil., University Professor, Nicolaus Copernicus University in Toruń, Faculty of Political Science and International Studies, Stefana Batorego 39L, 87-100 Toruń, Poland.

alone, including romance scams and lottery or sweepstakes scams. This amount represents an 11% increase compared to the previous year, with an average loss of about $34,000 per senior victim, and nearly 6,000 victims losing over $100,000, often wiping out their life savings.[1] In 2024, losses among Americans over 60 rose further, with reported losses reaching $4.8 billion, accounting for over 25% of total internet crime losses, and an average loss per victim of $83,000 – more than four times the overall average loss.[2] Fragmentary and often incomplete data also indicate an increase in this phenomenon in other countries. For example, in Poland, one of the most common crimes committed against the elderly involves fraud schemes known as the "grandson" and "policeman" methods. It is indicated that nearly 80% of the victims are people over 70 years of age.[3] These crimes are particularly severe because seniors often lose their entire life savings. In Spain, one of the most common digital crimes is fraud, which includes activities such as phishing – the malicious practice of impersonating another person or entity to obtain passwords, personal data or access to bank accounts. According to the System of Crime Statistics (SEC), managed by the Ministry of Home Affairs, 88% of all cybercrimes reported in 2019 corresponded to online fraud.[4] According to figures from the UK's Fraud and Cybercrime Centre Action Fraud, there were more than 13,500 reported cases of online fraud targeting people aged 60 and over in England

[1] Portal Radia Deon, *W 2023 roku seniorzy w USA stracili ponad 3 mld USD na skutek oszustw*, 2.5.2024, https://deon24.com/2024/05/02/w-2023-roku-seniorzy-w-usa-stracili-ponad-3-mld-usd-na-skutek-oszustw (access: 20.8.2025). See also FBI, *Elder Fraud*, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/elder-fraud (access: 20.8.2025). It is also reported that senior citizens are less likely to report fraud. This is supported by figures from the FTC, which show that while 44% of younger people aged 20–29 reported losing money to fraud, only 20% of elderly people aged 70–79 did the same. The FBI speculates that this may be due to a lack of understanding of the reporting process. See more R. Walsh, P. Bischoff, *US Cyber Security and Cybercrime Statistics*, 10.1.2024, https://www.comparitech.com/blog/information-security/us-cyber-crime-statistics (access: 20.8.2025); M. Gill, R. Walsh, *Senior Scam Statistics*, 16.1.2024, https://www.comparitech.com/identity-theft-protection/senior-scam-statistics (access: 20.8.2025).

[2] Monitor, *FBI alarmuje: Amerykanie stracili rekordowe 16,6 mld dolarów w 2024 roku w wyniku przestępstw internetowych*, 23.4.2025, https://www.monitorlocalnews.com/fbi-alarmuje -amerykanie-stracili-rekordowe-16-6-mld-dolarow-w-2024-roku-w-wyniku-przestepstw-internetowych (access: 20.8.2025).

[3] See more A. Rymsza, *Seniorzy są łatwym celem oszustw w Internecie. Trzeba zadbać o ich edukację!*, 13.11.2019, https://www.dobreprogramy.pl/seniorzy-sa-latwym-celem-oszustw-w-internecie-trzeba-zadbac-o-ich-edukacje,6628728443115137a (access: 20.8.2025). In 2022, as many as 3,500 seniors over the age of 65 fell victim to scams such as the "grandchild scam", "police scam" or "official scam", resulting in financial losses exceeding PLN 141 million. See D. Jaroszewski, *Polscy seniorzy masowo się na to nabierają. Straty sięgają 141 mln zł*, 28.12.2023, https://www.telepolis.pl/tech/bezpieczenstwo/oszustwo-wnuczek-nask-statystyki (access: 20.8.2025).

[4] M. Pascual, *Las estafas por internet representan más del 80% de los ciberdelitos*, 6.8.2021, https://www.newtral.es/estafas-internet-ciberdelitos/20210806 (access: 20.8.2025).

and Wales between April and September 2019 alone.[5] Whether through phishing emails, fake invoices or phone tech support calls, scammers are targeting people who, in some cases, are the most vulnerable. The above examples already illustrate the scale of the problem. However, accurately measuring the scale of internet fraud is beyond the cognitive capabilities of criminology.[6]

In most frauds, perpetrators take advantage of gullibility and lack of vigilance, especially among elderly and lonely people. Scammers play with their feelings and manipulate them. In practice, it is easier to convince elderly, single people and retirees that if they pay a certain amount of money, they will receive a pension supplement. Fraudsters very often rely on ignorance and try to take advantage of it by claiming that, thanks to money from the European Union, the apartment's water or gas installation will be renovated.

Using the Internet to commit fraud is definitely cheaper and, at the same time, more difficult to detect than traditional methods of criminal activity. The Internet provides the opportunity to reach a much larger number of potential victims and creates new opportunities to commit a wide range of frauds, such as publishing false information on websites created for this purpose or fraudulent trading via online portals. According to the most recent Eurostat data from 2024, Internet use among people aged 16 to 74 in the European Union has increased significantly compared to 2020. In 2024, 93% of individuals in this age group reported having used the Internet in the previous 3 months. Focusing on older adults aged 65 to 74, 59% of them used online banking in 2024.[7]

---

[5] D. Palmer, *Cybersecurity: Why More Needs to Be Done to Help Older People Stay Safe Online*, 12.11.2019, https://www.zdnet.com/article/cybersecurity-why-more-needs-to-be-done-to-help-older-people-stay-safe-online (access: 20.8.2025).

[6] The amount of information about the characteristics of criminals and victims of fraud on the Internet is very limited. In particular, the lack of instruments that would enable research in this area means that official publications on crime statistics usually omit not only information about the characteristics of criminals and victims, but also additional data regarding, among others, the means used by the perpetrator to commit them. The phenomenon of fraud on the Internet is extremely dynamic, and the diversity of forms and methods of operation of perpetrators of cybercrimes means that they often cannot be included in any control mechanism or properly categorized. Furthermore, the main difficulty in the process of examining the scale of fraud against elderly people in online commerce and electronic banking is access to reliable sources of research material. In this respect, what is particularly noticeable is the lack of uniform statistics and qualitative data, the lack of public availability of police data and the unreliability of data from entities dealing with security protection in computer systems and networks, including due to the fact that they are often collected and compiled for their benefit. This is mainly the result of a larger problem related to the estimation of cybercrime, in which it is indicated that most countries currently have insufficient and ineffective data collection mechanisms, which at best allow only a partial picture of the scale of the analyzed phenomenon to be obtained, which is at the same time burdened with a large statistical error.

[7] See Eurostat, *Digitalisation in Europe – 2025 Edition*, https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025 (access: 20.8.2025); Eurostat, *People Online in 2024*, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241217-1 (access: 20.8.2025).

Given this context, a crucial question arises: How can criminal law effectively protect older adults against various types of online fraud? Understanding the diverse definitions of fraud and the modus operandi of perpetrators is essential. Analyzing legal solutions adopted in different countries can help assess whether current protections are adequate. While each country decides on special protections for seniors, international cooperation and harmonization of laws are increasingly necessary to combat cross-border cybercrime effectively. Taking into account the diversity of definitions of fraud, it is worth paying attention not only to the colloquial understanding of the concept, but also to the legal definitions. It is also important to consider the modus operandi of the perpetrators of internet fraud.[8] This will help to understand, at least in part, why elderly people are so often victims of scammers. Then, it is worth analyzing the solutions adopted in selected countries. This will allow us to assess whether the legal solutions adopted in those countries adequately protect elderly people against online fraud. Of course, the decision to grant special protection to elderly people is always the responsibility of each country. However, with the widespread automation of ICT networks and systems and the dynamic development of cross-border services provided electronically, it seems necessary to be open to model foreign solutions worth adopting and disseminating. Also, in the era of universal access to the borderless Internet, it is necessary to adopt similar legal solutions in as many countries as possible. This will at least make it more difficult for perpetrators to choose the place of attack because of more favorable legislation (so-called forum shopping).

It is obvious that the purpose of criminal proceedings should not be to assess the implementation of civil-law contracts or to interpret their content. Furthermore, not every improper performance of a contract, even if it concerns financial or material matters, should lead to criminal liability. The same applies to various types of problems and difficulties in settling mutual obligations in e-commerce, which always involves a certain risk. Against this background, the second question arises: Should the understanding of fraud also include the conscious use of the gullibility, ignorance or misunderstanding of elderly people?

[8] The choice of countries whose legislation has been analyzed is based mainly on the desire to show the solutions to the crime of fraud applicable in neighbouring countries from Poland. The provisions in force in the countries of England, Wales and Northern Ireland and the United States of America are also worth attention due to the solutions adopted there, which are interesting from the point of view of a continental lawyer.

RESEARCH AND RESULTS

In colloquial terms, fraud is generally understood as an intentional and deceptive violation of the accepted rules of social coexistence (e.g. breaching established norms in business transactions) undertaken to gain an undue advantage by causing another person to their detriment. The primary aim of such manipulation is usually to obtain financial benefit for the perpetrator, although other advantages may also be sought, such as increased prestige, reputation, improved creditworthiness or political gain.

Dictionaries commonly define fraud as deliberately misleading another person to secure an undue advantage. For instance, the Polish dictionary describes fraud as intentionally deceiving someone or exploiting another's mistake for personal gain.[9] Similar definitions appear in foreign-language dictionaries. For example, *Black's Law Dictionary* characterizes fraud as a general term encompassing various behaviors resulting from human ingenuity, aimed at gaining an advantage over another by creating a false impression or limiting access to the truth. Fraud includes a wide range of tricks, deceptions, pretenses and other unfair means used to mislead others. Accordingly, *Black's Law Dictionary* categorizes fraud into types such as actual fraud, bank fraud, bankruptcy fraud, criminal fraud and other fraudulent acts.[10]

This broad definition is advantageous because it covers behaviors classified as fraud regardless of whether they result in property damage, personal injury or limit the victim's ability to achieve their goals. Based on this understanding, scholars classify fraud into: misrepresentation of material facts or false pretenses, concealment of material facts, bribery, extortion, conflicts of interest, forgery, embezzlement, theft and breach of fiduciary duty.[11]

Fraud is often regarded as a white-collar crime, typically committed by respected individuals or those holding significant social positions who exploit their reputation or status to commit offenses. It is also a key element of corporate crime (occupational or corporate crime), involving enrichment at the expense of a company or for its benefit by employees.

In practice, the broad scope of fraud can lead to divergent interpretations. Particularly in business, the same conduct may be viewed by some as intellectual skill, by others as a tort giving rise to civil liability, and by yet others as a criminal offense. This includes violations of contractual provisions, business guidelines, in-

[9] A. Bańkowski, *Etymologiczny słownik języka polskiego*, vol. 2, Warszawa 2000, p. 457; E. Sobol, *Słownik języka polskiego*, Warszawa 2005, p. 623.

[10] Association of Certified Fraud Examiners, *Fraud Examiners Manual*, 2009, http://thelawdictionary.org/fraud (access: 20.8.2025), p. 2201.

[11] J.T. Wells, N.S. Bradford, G. Geis, J.D. Gill, W.M. Kramer, J.D. Ratley, J. Robertson, *Fraud Examiners Manual*, Austin 2011, p. 670.

ternal policies and workplace regulations. A notable example from Poland involves fraud in the sale of so-called "miraculous" pots and kitchen utensils to elderly consumers. Victims were misled about the price and quality of the products. Initially, these actions were not classified as fraud because the elderly had the opportunity to read the contracts they signed. However, later scrutiny focused on the manner in which the goods were presented and the terms of purchase. During resort shows, pensioners were often pressured into signing multiple documents, some of whom were unaware that they had entered into loan agreements with exorbitant interest rates.[12] This case illustrates that fraud can take the form not only of false statements but also of manipulation and exploitation of vulnerable groups, blurring the line between aggressive sales tactics and criminal conduct.

Fraud, although defined differently around the world, shares several common features that distinguish it from legitimate business activities. Fundamentally, fraud always involves intentional deception or misrepresentation aimed at obtaining an unfair or unlawful advantage at the expense of another person or entity. Often, perpetrators are individuals who enjoy trust or hold significant social status, exploiting their reputation or position to deceive victims. A key element of fraud is the pursuit of illegal enrichment, which sets it apart from ordinary business risk-taking. Moreover, fraud violates legal and ethical norms, crossing the boundaries of acceptable commercial conduct.

1. Characteristics of fraud on the Internet

The increase in fraud crimes against elderly people on the Internet can be attributed to several factors. The literature on the subject indicates that the basic cause is mainly due to the cognitive deterioration of elder adults (systemic decline in memory, processing speed, problem-solving ability, mathematical skills, linguistic ability and executive function),[13] while physical decline, increased loneliness and fear of ageing also weaken cognitive ability among elder adults (social isolation). Another general reason is that older adults are more easily fooled than younger people because they are more likely to trust others. It has been pointed out that elder adults tend to have a higher level of trust, especially in their friends, neighbours and relatives, reducing their social defense mechanism.[14] Naturally, the level of

[12] C. Hlavica, U. Klapproth (eds.), *Tax Fraud & Forensic Accounting. Umgang mit Wirtschaftskriminalität*, Wiesbaden 2011, pp. 86–88.

[13] A. Vishwanath, T. Herath, R. Chen, J. Wang, H.R. Rao, *Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model*, "Decision Support Systems" 2011, vol. 51(3), pp. 576–586.

[14] J. Shao, W. Du, T. Lin, X. Li, J. Li, H. Lei, *Credulity Rather Than General Trust May Increase Vulnerability to Fraud in Older Adults: A Moderated Mediation Model*, "Journal of Elder Abuse & Neglect" 2019, vol. 31(2), pp. 146–162.

trust in elder adults is also influenced by other characteristics related to personality. Researchers also discovered relationships between other personality characteristics of the older population and their susceptibility to fraud. These personality traits include the "Big Five", self-control and social loneliness.[15] Furthermore, elder individuals may be less familiar with the complexities of online technology and may not fully understand the risks involved, making them more susceptible to scams and fraud (technical factors and empirical knowledge factors). One finding indicated, e.g., that older adults were less familiar and comfortable with computers and smartphones, and had lower self-efficacy in the use of them than younger people, which may reflect a lack of understanding of the Internet.[16] Research also found that the fraud techniques used by scammers are mainly focused on stimulating the victim's instincts.[17] Although the opinions mentioned above seem rational, there are no detailed studies that would show that elderly people are more susceptible to fraud than other groups of people. Current researchers are focused more on why older adults are easy targets for fraud.

Scammers often target specific vulnerabilities, such as offering fake medical cures to exploit health concerns or posing as family members in distress to emotionally manipulate elder individuals. They use various forms of social engineering to manipulate and deceive elderly people into sharing personal and financial information. In all these cases, a "computer" is a tool of crime serving the perpetrator as a communication channel, a tool enabling access to information or a tool for disseminating phishing communications. For example, by using a "false" website, the perpetrator may offer the possibility of quick profits from investments in "non-existent" companies or spread false information (e.g. in the form of forged or counterfeit press reprints) aimed at influencing the amount of the company's shares. A group of such frauds that can only be committed on the Internet can be broadly referred to as internet fraud.[18]

In the so-called identity fraud, the perpetrator uses another person's personal information, without authorization, to commit to deceive or defraud other person,

[15] Y. Shang, Z. Wu, X. Du, Y. Jiang, B. Ma, M. Chi, *The Psychology of the Internet Fraud Victimization of Older Adults: A Systematic Review*, "Frontiers in Psychology" 2022, vol. 1.

[16] P. Fischer, S.E. Lea, K.M. Evans, *Why Do Individuals Respond to Fraudulent Scam Communications and Lose Money? The Psychological Determinants of Scam Compliance*, "Journal of Applied Social Psychology" 2013, vol. 43(10), pp. 2060–2072.

[17] Y. Shang, Z. Wu, X. Du, Y. Jiang, B. Ma, M. Chi, *op. cit*. In this text, the authors present a broader literature and make a detailed analysis.

[18] On the other hand, a fraudulent attack may target not only the individual but also the system, data and computer programmes involved in the process of processing, collecting or transmitting computerised monetary deposits. See M. Siwicki, *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018.

e.g. by misleading the identity of the payment beneficiary.[19] Identity fraud is usually part of a practice of "fishing" for confidential personal information, passwords, PIN or one-time code (TAN), known as phishing.

In the case of the "grandchild" method (based on family ties and the natural need to help loved ones in an emergency), perpetrators during the initial conversation are trying to find out whether the person they are talking to may become their "victim" or not. They try to make the elder person feel that he or she should help his or her grandson or granddaughter at all costs and as quickly as possible. These feelings are much stronger than rational thoughts that warn of danger. In other scenarios, criminals play the role of an employee of the social insurance institution, bank, environmental protection office, tax chamber, etc., and cynically exploit the financial needs of their potential "victims". The elderly people hearing, e.g., about the possibility of obtaining larger benefits or nonrepayable financial assistance, "missing payment" in exchange for the benefits offered, e.g. pension indexation, connection of a gas or photovoltaic installation, furnace replacement. Perpetrators of identity fraud often also take advantage of various types of natural disasters and other tragic events by posing as victims in order to obtain "help" from various types of government and nonprofit organizations.

Generally, the perpetrator's modus operandi of identity theft (or identity fraud) can be divided into two stages. The first involves preparation by obtaining the necessary information. The obvious goal of the perpetrator of identity theft is to collect enough information about a person to be able to impersonate him or her (e.g. using various types of websites, banking and financial services, online stores or online transaction platforms). Then, the information obtained by the perpetrator can be used to commit classic fraud, e.g. by impersonating the person whose data he obtained, or, among others, to take over an online bank account and change the beneficiary of the transaction.[20]

Another form, which is the simplest and at the same time most effective form of online fraud, is offering to sell non-existent goods or misleading as to such circumstances as the quantity, quality or properties of a given item sold at online auctions or in online stores. In this case, the perpetrator relies on the specific nature of the Internet and the conclusion of contracts that use it. A person who, e.g., bids on goods at an online auction cannot see them or take them with them after the transaction, and the seller does not receive payment directly. For these reasons, at least three types of fraud are possible in online auctions: failure to send the goods or

[19] United Kingdom, Cabinet Office, *Identity Fraud: A Study*, July 2022, https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-fraud-study (access: 20.8.2025).

[20] See M. Siwicki, *Prawo karne…*, pp. 38–71. In this text, the author present a broader literature and make a detailed analysis.

failure to pay; sending a different product or one with a lower value than the agreed one; failure to disclose all relevant information about the product or terms of sale.[21]

Another type of fraud, more complex than the previous ones, is the so-called investment fraud, in which the perpetrator, usually using email, misled the recipient of the message as to the existence of a good or bad financial condition of a given entity or whether it had a specific right. The perpetrator may, e.g., offer the possibility of quick profit from investments in "trusted" companies, disseminate false information (e.g. in the form of forged or counterfeit press reprints) aimed at influencing the amount of the company's shares (so-called trash and cash schemes). However, the most characteristic symbol of the so-called investment fraud on the Internet is the so-called Nigerian scam (also known as the Nigerian 419 scam).[22] Most often, it begins with establishing contact via email with a potential victim (formerly random, now more and more frequently selected) and offering him or her the possibility of obtaining significant funds (e.g. part of the fortune that the fraudster has or inherited, part of the profits from an investment, from a winnings lottery, etc.), instead of for "help" in recovering them, consisting in, e.g., opening and authenticating a bank account, paying a bribe, court costs or finalizing other steps that the fraudster must complete to finalize the fictitious transfer of funds to the indicated account by the victim. However, only the fraudster takes over the money paid by the victim, who, from time to time, makes the fraud plot more credible by sending prepared certificates, copies of transfer confirmations, etc., by email.

Equally often, the perpetrator may mislead about various phenomena and events. For example, a type of investment fraud called "pump-and-dump scam"[23] consists of the perpetrator purchasing practically worthless shares and using various techniques to artificially inflate the price of a single share, e.g. by spreading a rumor on the Internet that a joint-stock company is to be bought out in the near future or receive a significant contract, or the use of investment bulletins that are supposed to appear to be objective studies, but in fact their purpose is to mislead the injured party, e.g. as to the financial situation of a specific entrepreneur.

There are many factors that contribute to the increase in the number of frauds on the Internet. One of the fundamental issues seems to be the increase in the availability of telecommunications and information technologies, which has significantly increased the possibility of using the achievements of new technologies for criminal

[21] Cf. J. Clough, *Principles of Cybercrime*, New York 2010, pp. 183–199; C. Chin, *Cybercrime and Cyberfraud*, [in:] *The Internet Encyclopedia*, ed. H. Bidgoli, vol. 1, Hoboken 2004, pp. 331–332.

[22] P. Bischoff, *What Is the Nigerian Scam (419 Scam) with Examples*, 22.9.2023, https://www.comparitech.com/identity-theft-protection/nigerian-scam (access: 20.8.2025).

[23] For example, see M. La Morgia, A. Mei, F. Sassi, J. Stefa, *Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations*, 2020, https://ieeexplore.ieee.org/document/9209660 (access: 20.8.2025); Investopedia, *How Does a Pump-and-Dump Scam Work?*, 13.1.2022, https://www.investopedia.com/ask/answers/05/061205.asp (access: 20.8.2025).

purposes and obtaining profits in previously inaccessible areas. The reasons for the increase in the number of frauds on the Internet should also be sought in the lack of trust of internet users in law enforcement agencies due to the low effectiveness of their actions, which translates into frequent resignation by victims from filing reports of harm.[24]

Internet fraud also presents numerous forensic challenges, particularly in gathering evidence of the perpetrator's guilt. These challenges include the frequent lack of material evidence, limited understanding of the technologies used by criminals and the need to rely on expert opinions from computer scientists. Prosecution is further complicated by the anonymous nature of the Internet, jurisdictional issues (as criminals often operate internationally), the deliberate concealment of evidence by perpetrators, lack of cooperation from victims (who may fear legal consequences or embarrassment), rapidly evolving technologies and complex legal procedures. Legal regulations may also vary between jurisdictions, adding further confusion and difficulty to prosecuting online fraud.

Effective prevention and education are crucial in protecting elderly people from online fraud. Modern technologies also play a vital role in safeguarding older adults. Tools like anti-phishing filters, two-factor authentication and real-time bank alerts provide technical barriers against fraudsters. For example, banks increasingly use biometric verification and AI-driven fraud detection systems to identify suspicious transactions early and prevent losses. Moreover, user-friendly security software tailored for seniors can reduce their vulnerability by simplifying safe internet use.[25] Additionally, cross-border cooperation and harmonization of legal frameworks remain essential to address the transnational nature of cybercrime targeting elderly populations.

2. Perspective on comparative law

In any country with a developed capitalist economy, there is no doubt that online fraud must be intensively combated. Effective counteracting this phenomenon requires, first of all, knowledge of the often-sophisticated modus operandi of the perpetrator, a precise definition of the phenomenon and detailed issues, without which recognition and detection, as well as collecting evidence of the crime, are particularly difficult. It can be observed that different legal conditions and cultural

[24] According to various studies, cybercrimes are among the least frequently reported types of crimes. Victims often refrain from reporting computer crimes to the police for fear of unwanted publicity. Overall, it is estimated that only 20% of all computer abuse is reported. See M. Siwicki, *Charakterystyka sprawcy i ofiary „cyberoszustwa"*, [in:] *Problemy bezpieczeństwa Europy i Azji*, eds. T. Ambroziak, A. Czwołek, S. Gajewski, M. Nowak-Paralusz, Toruń 2016, pp. 450–462.

[25] "Aktywny Senior" 2023–2024, no. 7, https://www.wib.org.pl/wp-content/uploads/2023/12/231215-aktywny-senior-07-2023-2024.pdf (access: 20.8.2025).

traditions cause the nature of fraud to show significant differences in comparative law. This obviously makes it difficult to prosecute cybercrime perpetrators that act fraudulently against elderly people.

In comparative law, especially in European countries where the development of jurisprudence was influenced by Roman law, it is usually assumed that fraud is intentionally misleading another person in order to obtain an unfair or illegal financial advantage or depriving him of his right.[26] However, there are significant differences in the regulations for fraud offenses in individual countries, mainly in their detailed content, although individual types of prohibited acts show general similarities.

The position that fraud can only be committed intentionally and that it constitutes a targeted crime, characterized by the goal of obtaining financial gain, is widely spread. For example, in Estonia, according to § 209 of the Estonian Criminal Code of 6 June 2001 (RT I 2001, 61, 364), fraud (*kelmus*) is the receipt of a financial advantage as a result of consciously (*teadvalt*) causing a misconception of existing facts.[27] In Bulgaria, according to Article 209 of the Bulgarian Criminal Code of 1 May 1968 (*незаконни измами*, Journal of Laws No. 26/02/04/1968), fraud is causing or maintaining aberration in somebody in order to obtain a financial advantage for oneself or another person, causing damage to the deceived person or another person.[28] Similarly in Spain, according to Article 248 (1) of the Spanish Criminal Code (*Código Penal*), classic fraud (*estafa*) is the use of deceit (defined as a conscious and deliberate act), for commercial purposes, to mislead another person into disposing of property.[29]

In the German Criminal Code (*Strafgesetzbuch*), where the offence of fraud (*Betrug*) is regulated in Division 2, titled "Fraud and embezzlement", in Section 263, the punishability of the crime of fraud is limited to its intentional commission, and the perpetrator must act in order to obtain an unlawful material advantage (*ein rechtswidrigen Vermögensvorteil zu verschaffen*).[30] As in Germany, in other countries attention is also paid to the additional criterion of the illegality of the perpetrator's behavior. For example, in Finland, in the repeatedly amended Crim-

[26] The prototype of the crime of fraud was the Roman "stellionatus", which, based on the use of falsehood, violated property and other property rights. See T. Oczkowski, [in:] *System Prawa Karnego*, vol. 9: *Przestępstwa przeciwko mieniu i gospodarcze*, ed. R. Zawłocki, Warszawa 2015, pp. 117–120.

[27] English translation: https://www.riigiteataja.ee/en/eli/522012015002/consolide (access: 20.8.2025).

[28] English translation: https://www.mlsp.government.bg/uploads/1/blgarsko-zakonodatelstvo/en/criminal-code.pdf (access: 20.8.2025).

[29] English translation: https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf (access: 20.8.2025).

[30] English translation: https://www.gesetze-im-internet.de/englisch_stgb (access: 20.8.2025).

inal Code of 1889 (Journal of Laws 39/1889, as amended), fraud, according to Section 1 of Chapter 36 "Fraud and other dishonesty", is behavior undertaken in order to obtain an unlawful financial advantage for yourself or another person or for the purpose of causing harm to others.[31] The requirement to cause damage has also been adopted in other countries, such as Spain (Article 248), Italy (Article 640), Switzerland (Article 146) and Poland (Article 286). But there are countries where fraud can be established without proving the actual harm or loss to the victim. Examples of countries where it is not necessarily required to cause harm include the Netherlands (Article 326b) or Sweden (Chapter 9 § 1), where fraud is defined as misleading others to gain a financial advantage. In practice, in these countries, it is easier to prove fraud because it is enough to prove that the perpetrator took a specific action, regardless of whether it results in damage.

In some countries, the fraudulent methods of committing fraud are defined in detail. For example, in Germany, causative action is defined as obtaining (purchasing) a financial advantage (*Vermögensvorteil zu verschaffen*) by misleading another person or exploiting (maintaining) his mistake. Misrepresentation may occur by means of false facts (*Vorspiegelung falscher Tatschen*), by concealment (*Unterdrückung*) or distortion of true facts (*Entstellung wahrer Tatsachen*). The perpetrator does not have to act only in order to obtain unlawful financial gain, but also with the intention of causing damage to another person.

Similar solutions were also adopted in Switzerland in Article 146 of the Swiss Criminal Code.[32] In this country, however, an additional condition is set that the perpetrator must "deceitfully" mislead (*arglistig irreführen*) or "deceitfully" take advantage of someone else's mistake (*arglistig einen Irrtum bestärken*).[33] The case law indicates that such fraudulent misrepresentation takes place, among others, when the perpetrator: has built a whole network of lies that prove his particular perversity, and the lies are matched to each other and are difficult to recognize, or the perpetrator has created false documents and certificates in order to make the fraud credible. At the same time, it is assumed that there is no fraud within the meaning of Article 146 if the victim, having exercised a minimum of due diligence, could have noticed the fraud, e.g. the victim did not take even the most basic precautions (BGE 126 IV 165 S. 173).[34] Also, under the Swedish Criminal Code, which

[31] English translation: https://www.finlex.fi/api/media/statute-foreign-language-translation/511348/mainPdf/main.pdf?timestamp=1889-12-19T00%3A00%3A00.000Z (access: 20.8.2025).

[32] English translation, status as of 1 September 2017: https://www.warnathgroup.com/wp-content/uploads/2017/11/Switzerland-Penal-Code-2017.pdf (access: 20.8.2025).

[33] English translation, status as of 1 July 2020: https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/54/757_781_799/20200701/en/pdf-a/fedlex-data-admin-ch-eli-cc-54-757_781_799-20200701-en-pdf-a.pdf (access: 20.8.2025).

[34] Available online: https://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F126-IV-165%3Ade&lang=de&type=show_document (access: 20.8.2025).

was adopted in 1962 and entered into force on 1 January 1965, it is assumed that fraud is the insidious inducement of another person to perform a specific behavior or omission, which results in the perpetrator receiving a profit, and on the side of the defrauded party or the person he represents, there is a loss. Providing false or incomplete information also constitutes fraud (Section 1). In other countries this additional feature is also introduced, e.g. e.g. Article 177 (1) of the Slovak Criminal Code defines the offense in its basic form, while Article 122 (6) refers to the qualified form of this offense (an offense committed by unlawful breaching of a lock or other security system, or by using deception, such as trickery or deceit), Section 177 (1) of the Latvian Criminal Code (use of bad faith, trust or by deceit[35]), Article 190 of the Ukrainian Criminal Code (deceit or breach of confidence[36]) and Article 248 the Spanish Criminal Code.

The difference in the distribution of accents in these cases is mainly related to the manner of action and the intention of the person participating in these actions. In the first case, the perpetrator must have proven a deliberate and conscious action in which a person acts with the intent to deceive others for the purpose of gaining an unlawful benefit, such as financial gain. In the latter case of the exploitation of error or ignorance, it is enough to prove that a person takes advantage of another's lack of knowledge or error, but not necessarily with the intent to defraud. In both cases, a violation of the law may occur, but the intent and purpose of the action are key differences.

In some countries, when defining the manner of committing fraud, reference is made to the specific characteristics of the person dealing with the property, including her inability to properly understand the undertaken action, both of a permanent nature (when the cause is, e.g., immaturity) and of a temporary nature (when the cause is, e.g., intoxication). For example, in France, according to Article 223-15-2 of the French Criminal Code of 1992, *escroquerie* is punishable to fraudulently abuse the recklessness or weakness of a minor or the special sensitivity of another person due to age, illness, infirmity, disability, mental retardation, or pregnancy, as well as people in a state of physical or mental dependence resulting from serious or repeated disorders. It is also punishable to use various types of fraudulent techniques to influence a person's assessment in order to induce him or her to act or refrain from taking a specific action. In the Bulgarian Criminal Code, according to Article 209 (2) (Amend. SG 10/93), it is also punishable to use the "lack of experience or lack of information of someone else". Similarly, in Finland, the qualified form is

[35] English translation: https://legislationline.org/sites/default/files/2023-10/Criminal%20Code%20of%20Latvia.pdf (access: 20.8.2025).

[36] English translation: https://sherloc.unodc.org/cld/uploads/res/document/ukr/2001/criminal-code-of-the-republic-of-ukraine-en_html/Ukraine_Criminal_Code_as_of_2010_EN.pdf (access: 20.8.2025).

provided for in situations when the perpetrator commits fraud "by taking advantage of a special weakness or other insecure position of another" (Aggravated fraud, Amend., 24 August 1990/769). It is also worth paying attention to the solutions adopted in Slovakia, where the qualified type of fraud, punishable by imprisonment of 2 to 8 years, is defined in § 221 (3) of the Criminal Code.[37] The qualifying features in this case are: significant damage resulting from the crime committed (pursuant to § 125 significant damage is a value that is at least 250,000 EUR), committing a crime with a special motivation, committing a crime in a particular way, and committing a crime to the detriment of the protected person.

The mark of committing a crime in a specific way was defined in the § 138 of the Slovak Criminal Code. From the point of view of the subject of the analysis of this article, the following circumstances may be relevant: committing a crime to the detriment of several people, committing a crime taking advantage of the helplessness, lack of experience, dependence, or subordination of another person, committing a crime in breach of the obligations imposed by law related to profession, function or position held. The scope of the concept of "protected person" is indicated in § 139 of the Slovak Criminal Code, and it is quite extensive. According to this provision, a protected person is, among others, a child, a pregnant woman, a close person, an elderly person, and a sick person.

Penalties for fraud also vary across Europe. In Finland and Sweden, the penalty for fraud is 2 years. In Estonia, fraud is punishable by imprisonment of up to 3 years. In Germany, fraud is punishable by up to 5 years in prison. In Austria, it is punishable by imprisonment of up to one year or a fine of up to 360 daily rates. In qualified types, the penalty obviously increases significantly. In the event of damage exceeding EUR 5,000, it is punishable by imprisonment for up to 3 years, and if the damage amounted to more than EUR 300,000, imprisonment from 1 to 10 years. In Switzerland, fraud is punishable by imprisonment for up to 5 years or a fine. However, if the fraud occurred as part of business activity, the penalty is up to 10 years in prison. Similarly, in France, fraud is punishable by up to 3 years in prison, and if it was committed by a person who abused his managerial position or by abusing another person's mental or physical dependence, the penalty increases to 5 years. In Bulgaria, fraud is punishable by 1 to 6 years of deprivation of liberty. In Poland, fraud is punishable by 8 years of deprivation of liberty, and Spain sets prison terms from 4 to 8 years depending on the amount involved and circumstances. These differences reflect varying legal traditions, the gravity assigned to fraud, and policy priorities regarding deterrence and rehabilitation.

A slightly different scheme of criminalization of fraud has been adopted, among others, in the criminal legislation of the countries of the Anglo-American system, which usually clearly distinguishes between the crime of fraud and the civil law

[37] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300 (access: 20.8.2025).

tort of deceit. Although the precise definitions of these concepts and the conditions for distinguishing them vary from country to country, it is usually assumed that:

1. In the case of fraud, special attention should be paid to the element of false representation, i.e. activities that are one-way communication (from the perpetrator to the victim) and the perpetrator's intention to obtain things (property, property rights) from another person using fraudulent treatments.
2. In the case of deception perceived primarily from the perspective of false representation, the active participation of the other injured party, misled by the perpetrator (two-way communication), is necessary. As R. Heaton points out, in the case of a civil law tort, the perpetrator intentionally misleads or conceals important facts, which contributes to the victim's perception of an unfavorable decision (e.g. concluding an unfavorable contract, selling goods at a lower price, etc.). This author emphasizes that, in the case of a tort, such insidious assurances must "get into the victim's mind".[38]

The distinction between these two concepts raises many problems in practice, especially in cases of an economic nature. This includes, among others, if one party fails to provide all the information it has, resulting in losses for the other party. As indicated in American doctrine, the obligation to disclose information will depend on the nature of the contract, and the line between business transactions and fraud may often be difficult to determine. For example, the doctrine, referring to the case of *Neil v. Shamburg* from 1983, indicates that the seller is obliged to notify the buyer of all hidden defects of the item sold, but on the other hand, the buyer has no legal obligation to notify the seller that the item sold is worth much more than the price asked by the seller. For these reasons, some authors even point out that parties should have the right to lie and hide information when it comes to unverifiable statements, personal opinions and judgments, and such behavior cannot be classified as fraud.[39]

In the U.S. federal statute governing fraud at 18 U.S.C. 1341,[40] it is assumed that, in the case of fraud crime, it is necessary to prove the existence of five elements: false presentation of an important fact by the perpetrator; awareness on the part of the perpetrator that such facts are untrue; the intention to defraud the alleged victim (e.g. deprive him of some entitlement); damage to the alleged victim as a result of the perpetrator's actions; acts to obtain money or property.

[38] R. Heaton, *Criminal Law: Textbook*, Oxford 2006, p. 327.

[39] M. Šepec, *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-Related Fraud: A Comparative Legal Analysis*, "International Journal of Cyber Criminology" 2012, vol. 6(2), pp. 984–1000.

[40] US Code – Code of Laws in the United States (A Comprehensive Code of the United States), http://www.law.cornell.edu/uscode (access: 20.8.2025).

The doctrine emphasizes that to assess whether fraud has occurred, it is also necessary to assess the gullibility of the injured party. The injured party's unjustified reliance on the perpetrator's absurd lies will not constitute fraud unless the perpetrator consciously took advantage of the victim's particular intellectual or emotional state.

In England, Wales and Northern Ireland, the Fraud Act 2006 provides for three types of fraud: false representation (Section 2); fraud by failing to disclose information (Section 3); fraud by abuse of position (Section 4).

The first type of fraud requires the following: knowingly presenting false or misleading facts, information or law; acting in order to make a profit for yourself or another person (to make a gain for yourself or another) or to cause loss to another or to expose another to a risk of loss.

The second type of fraud involves the perpetrator's conscious and dishonest failure to disclose information, contrary to his legal obligation, in order to gain profit for himself or another person or to cause or risk damage to another person.

Similarly, the third type involves the perpetrator's abuse of a position where he or she is expected to look after another person's financial interests, also in order to make a profit or cause damage to another person (or risk of harm).

Assessing the gullibility of the injured party as a factor in determining whether fraud has occurred is also required in the United Kingdom, where the concept of a "reasonable person" may be considered when determining whether the victim's gullibility or vulnerability contributed to the fraud. If the injured party acted incorrectly, carelessly or improperly, which contributed in some way to the fraud, it can affect whether the fraud is recognized. In the UK, the case of *Derry v Peek* (1889) LR 14 App Cas 337[41] and the case *Hedley Byrne & Co Ltd v Heller & Partners Ltd* (1964) AC 465[42] are typical in this respect.

As in Switzerland, mentioned above, in Ireland, under the 2001 Criminal Justice (Theft and Fraud Offences) Act, the offense of fraud requires "any deception". For the purposes of this Act, a person deceives if he or she: a) creates or reinforces a false impression, including a false impression about law, value, intention or other state of mind, b) prevents another person from acquiring information which would affect that person's judgment of a transaction, or c) fails to correct a false impression which the deceiver previously created or reinforced or which the deceiver knows to be influencing another to whom he or she stands in a fiduciary or confidential relationship.

[41] http://www.e-lawresources.co.uk/Derry-v-Peek.php (access: 20.8.2025).

[42] http://www.bailii.org/cgi-bin/markup.cgi?doc=/uk/cases/UKHL/1963/4.html (access: 20.8.2025).

DISCUSSION AND CONCLUSIONS

In recent years, the number of online fraud cases has increased dramatically and shows no signs of slowing down. Over time, perpetrators have adopted increasingly sophisticated methods and techniques, ranging from basic phishing attacks to the development of professional software and hardware tools. More recently, organized criminal enterprises have emerged, providing protection to cybercriminals and forming associations that diversify activities within a functional division of labor.

The rise in internet fraud not only increases risks for businesses, undermines the sense of security and raises transaction costs, but also damages interpersonal relationships by eroding trust among people. Another challenge in combating online fraud is the lack of a clear, universally accepted definition of what constitutes fraud. This ambiguity complicates efforts to tackle the problem, especially given its global and cross-border nature. Difficulties arise in various areas, including crime research and measurement, policy development, public education, victim assistance and the creation of common prevention methods. While standardized definitions can optimize countermeasures, they are not strictly necessary to address the issue. Moreover, the existence of multiple definitions on the international stage can lead to diverse approaches to the same problem, potentially offering valuable models for others to consider.

From a comparative law perspective, it is evident that the concept of fraud encompasses a wide range of perpetrator behaviors, which may be tolerated or criminalized depending on the legal system. Unlike theft or misappropriation, which always involve financial gain for the perpetrator or another party, fraud does not necessarily require such benefit to occur. In many common law countries, the voluntary transfer of property by the victim is not always a defining element of fraud. Additionally, whether the victim could have detected the deception with reasonable care may influence the assessment of the crime. The victim's degree of gullibility or negligence can also be relevant. A common feature across jurisdictions is that perpetrators intentionally present false or misleading information to a specific person (creating a false impression) with the aim of obtaining unlawful financial gain for themselves or others.

These examples highlight significant differences in legal approaches to fraud protection. It is generally easier to protect older adults in countries where proving the victim's negligence or the perpetrator's intent is not required. To curb the rise of fraud crimes targeting the elderly, it is worth considering legal provisions that impose harsher penalties for exploiting specific vulnerabilities. While the core element of fraud – intentional deception to obtain an unlawful benefit – is universally recognized, jurisdictions differ in how they categorize fraud, the scope of acts considered fraudulent and the required elements such as intent and harm. Some countries emphasize the monetary value involved, using thresholds to de-

termine severity and penalties, while others focus on the method of deception or the relationship between parties. Additionally, legal systems vary in distinguishing between criminal fraud and civil wrongs, with some treating certain fraudulent acts primarily as civil matters and others as serious criminal offenses. These differences influence not only the legal definitions but also enforcement practices, prosecution standards and available sanctions.

Given the millions of scam victims annually, it is urgent to identify the factors that make older adults more susceptible to fraud and, importantly, to develop effective preventive measures. There is a growing need for theoretical frameworks that integrate cognitive science, neurology and personality research to better understand susceptibility to fraud among seniors. Since little is known about how to reduce internet fraud effectively, further interdisciplinary research is essential to develop decision aids and other tools to mitigate this problem. Although many online resources offer valuable advice, many elderly individuals do not follow these recommendations. Due to the complexity of the issue, closer collaboration among researchers from diverse fields, such as computer science and psychology, is likely to yield fruitful results. It also seems justified to consider legislative reforms to combat internet fraud, including harmonization of laws within the European Union and the adoption of special protections for older adults.

Effective prevention of online fraud against elderly people requires limiting the physical possibility of committing such crimes through various hardware and software security measures and depriving perpetrators of the technical tools they use. Equally important is increasing the risk of detection and conviction. Achieving this requires detailed analysis of specific crime forms, including data collection on their nature and scope. In the context of fraud targeting seniors, it is reasonable to focus on the conditions that enable or facilitate these crimes and systematically restrict them. Such efforts should prioritize establishing appropriate supervision and control systems, defining clear rules for computer system access and implementing thorough monitoring and user identification. The primary goal is to prevent perpetrators from concealing their identity and location.

Finally, combating internet fraud must go beyond state actions and involve international cooperation, public education and awareness-raising. Collaboration with internet service providers and end users, such as promoting self-regulation and digital literacy, is essential for effective prevention. Digital literacy programs tailored for seniors, combined with user-friendly security software and tools like two-factor authentication, anti-phishing filters and real-time fraud alerts, can significantly reduce vulnerability. Raising awareness among seniors and their families about common scams and safe online practices is equally important to empower them against fraud attempts.

REFERENCES

Literature

Bańkowski A., *Etymologiczny słownik języka polskiego*, vol. 2, Warszawa 2000.

Chin C., *Cybercrime and Cyberfraud*, [in:] *The Internet Encyclopedia*, ed. H. Bidgoli, vol. 1, Hoboken 2004, **DOI: https://doi.org/10.1002/047148296X.tie030**.

Clough J., *Principles of Cybercrime*, New York 2010, **DOI: https://doi.org/10.1017/CBO9780511845123**.

Fischer P., Lea S.E., Evans K.M., *Why Do Individuals Respond to Fraudulent Scam Communications and Lose Money? The Psychological Determinants of Scam Compliance*, "Journal of Applied Social Psychology" 2013, vol. 43(10), **DOI: https://doi.org/10.1111/jasp.12158**.

Heaton R., *Criminal Law: Textbook*, Oxford 2006.

Hlavica C., Klapproth U. (eds.), *Tax Fraud & Forensic Accounting. Umgang mit Wirtschaftskriminalität*, Wiesbaden 2011, **DOI: https://doi.org/10.1007/978-3-8349-6444-1**.

Shang Y., Wu Z., Du X., Jiang Y., Ma B., Chi M., *The Psychology of the Internet Fraud Victimization of Older Adults: A Systematic Review*, "Frontiers in Psychology" 2022, vol. 13, **DOI: https://doi.org/10.3389/fpsyg.2022.912242**.

Shao J., Du W., Lin T., Li X., Li J., Lei H., *Credulity Rather Than General Trust May Increase Vulnerability to Fraud in Older Adults: A Moderated Mediation Model*, "Journal of Elder Abuse & Neglect" 2019, vol. 31(2), **DOI: https://doi.org/10.1080/08946566.2018.1564105**.

Siwicki M., *Charakterystyka sprawcy i ofiary „cyberoszustwa"*, [in:] *Problemy bezpieczeństwa Europy i Azji*, eds. T. Ambroziak, A. Czwołek, S. Gajewski, M. Nowak-Paralusz, Toruń 2016.

Siwicki M., *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018.

Sobol E., *Słownik języka polskiego*, Warszawa 2005.

Šepec M., *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-Related Fraud: A Comparative Legal Analysis*, "International Journal of Cyber Criminology" 2012, vol. 6(2).

Oczkowski T., [in:] *System Prawa Karnego*, vol. 9: *Przestępstwa przeciwko mieniu i gospodarcze*, ed. R. Zawłocki, Warszawa 2015.

Vishwanath A., Herath T., Chen R., Wang J., Rao H.R., *Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model*, "Decision Support Systems" 2011, vol. 51(3), **DOI: https://doi.org/10.1016/j.dss.2011.03.002**.

Wells J.T., Bradford N.S., Geis G., Gill J.D., Kramer W.M., Ratley J.D., Robertson J., *Fraud Examiners Manual*, Austin 2011.

Online sources

"Aktywny Senior" 2023–2024, no. 7, https://www.wib.org.pl/wp-content/uploads/2023/12/231215-aktywny-senior-07-2023-2024.pdf (access: 20.8.2025).

Association of Certified Fraud Examiners, *Fraud Examiners Manual*, 2009, http://thelawdictionary.org/fraud (access: 20.8.2025).

Bischoff P., *What Is the Nigerian Scam (419 Scam) with Examples*, 22.9.2023, https://www.comparitech.com/identity-theft-protection/nigerian-scam (access: 20.8.2025).

Eurostat, *Digitalisation in Europe – 2025 Edition*, https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025 (access: 20.8.2025).

Eurostat, *People Online in 2024*, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20241217-1 (access: 20.8.2025).

FBI, *Elder Fraud*, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/elder-fraud (access: 20.8.2025).
Gill M., Walsh R., *Senior Scam Statistics*, 16.1.2024, https://www.comparitech.com/identity-theft-protection/senior-scam-statistics (access: 20.8.2025).
Gill M., Walsh R., *Senior Scam Statistics*, 16.1.2024, https://www.comparitech.com/identity-theft-protection/senior-scam-statistics (access: 20.8.2025).
Investopedia, *How Does a Pump-and-Dump Scam Work?*, 13.1.2022, https://www.investopedia.com/ask/answers/05/061205.asp (access: 20.8.2025).
Jaroszewski D., *Polscy seniorzy masowo się na to nabierają. Straty sięgają 141 mln zł*, 28.12.2023, https://www.telepolis.pl/tech/bezpieczenstwo/oszustwo-wnuczek-nask-statystyki (access: 20.8.2025).
La Morgia M., Mei A., Sassi F., Stefa J., *Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations*, 2020, https://ieeexplore.ieee.org/document/9209660 (access: 20.8.2025).
Monitor, *FBI alarmuje: Amerykanie stracili rekordowe 16,6 mld dolarów w 2024 roku w wyniku przestępstw internetowych*, 23.4.2025, https://www.monitorlocalnews.com/fbi-alarmuje-amerykanie-stracili-rekordowe-16-6-mld-dolarow-w-2024-roku-w-wyniku-przestepstw-internetowych (access: 20.8.2025).
Palmer D., *Cybersecurity: Why More Needs to Be Done to Help Older People Stay Safe Online*, 12.11.2019, https://www.zdnet.com/article/cybersecurity-why-more-needs-to-be-done-to-help-older-people-stay-safe-online (access: 20.8.2025).
Pascual M., *Las estafas por internet representan más del 80% de los ciberdelitos*, 6.8.2021, https://www.newtral.es/estafas-internet-ciberdelitos/20210806 (access: 20.8.2025).
Portal Radia Deon, *W 2023 roku seniorzy w USA stracili ponad 3 mld USD na skutek oszustw*, 2.5.2024, https://deon24.com/2024/05/02/w-2023-roku-seniorzy-w-usa-stracili-ponad-3-mld-usd-na-skutek-oszustw (access: 20.8.2025).
Rymsza A., *Seniorzy są łatwym celem oszustw w Internecie. Trzeba zadbać o ich edukację!*, 13.11.2019, https://www.dobreprogramy.pl/seniorzy-sa-latwym-celem-oszustw-w-internecie-trzeba-zadbac-o-ich-edukacje,6628728443115137a (access: 20.8.2025).
United Kingdom, Cabinet Office, *Identity Fraud: A Study*, July 2022, https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-fraud-study (access: 20.8.2025).
Walsh R., Bischoff P., *US Cyber Security and Cybercrime Statistics*, 10.1.2024, https://www.comparitech.com/blog/information-security/us-cyber-crime-statistics (access: 20.8.2025).

Legal acts

Criminal Code of Bulgaria (2017). SG No. 85/24.10.2017.
Criminal Code of Estonia (2001). RT I 2001, 61, 364.
Criminal Code of Finland (2022).
Criminal Code of France (2024).
Criminal Code of Germany (2018). BGBl. 2024 I Nr. 109.
Criminal Code of Italy (2018).
Criminal Code of Latvia (2023).
Criminal Code of the Netherlands (2012).
Criminal Code of Poland (1997). Consolidated text, Journal of Laws 2024, item 17.
Criminal Code of the Republic of Ukraine (2001).
Criminal Code of Slovakia (2019). 474/2019 Coll.
Criminal Code of Spain (2024). Organic Law 10/1995, of 23 November, 33987-34058.
Criminal Code of Sweden (2020). SFS 1962:700 Brottsbalken.
Criminal Code of Switzerland (2020). StGB, SR 311.0.

ABSTRAKT

W ostatnich latach odnotowano dramatyczny wzrost cyberprzestępstw wymierzonych w seniorów. W krajach takich jak Polska rozpowszechniły się specyficzne metody oszustw, takie jak „na wnuczka" czy „na policjanta", a także ataki phishingowe, które często prowadzą do utraty oszczędności całego życia. Pomimo rosnącej skali problemu kryminologia napotyka trudności w dokładnym pomiarze zakresu oszustw internetowych. Zasięg i anonimowość Internetu ułatwiają popełnianie tych przestępstw, co sprawia, że ich wykrywanie i zapobieganie są trudniejsze niż w przypadku tradycyjnych metod. To rodzi istotne pytania dotyczące adekwatności obecnych rozwiązań prawnych chroniących osoby starsze oraz tego, czy prawo karne powinno uwzględniać wykorzystywanie ich łatwowierności lub niewiedzy. Analizując definicje prawne, modus operandi sprawców oraz porównawcze rozwiązania międzynarodowe, autor opracowania ma na celu ocenę, czy istniejące ramy prawne wystarczająco chronią seniorów oraz zbadanie potencjału harmonizacji ponadnarodowych środków prawnych, które mogłyby skuteczniej zabezpieczyć tę coraz częściej atakowaną grupę społeczną.

Słowa kluczowe: osoby starsze; oszustwa internetowe; prawo porównawcze; cyberprzestępczość