

# Protecting elderly people from online fraud. Comparative Law Aspects (iThenticate Similarity Report)

## **Protecting elderly people from online fraud. Comparative Law Aspects**

### **ABSTRACT**

This study is devoted to an analysis of how elderly people are protected against various types of fraud on the Internet in comparative law. The considerations devoted to this issue begin with an analysis of the concept of fraud, then the most common methods of fraud on the Internet directed against elderly people are presented, as well as the reasons for the increase in this trend of crime. The most important part of the study is, of course, the comparative legal analysis of solutions adopted in selected countries. Based on the above findings, in the conclusion an attempt was made to indicate possible actions that should contribute to limiting the scale of the increase in frauds directed against elderly people.

**Keywords: elderly people, online fraud, comparative law, cybercrime**

Niniejszy artykuł poświęcony jest analizie ochrony osób starszych przed różnymi rodzajami oszustw internetowych w prawie porównawczym. Rozważania na ten temat rozpoczynają się od analizy pojęcia oszustwa, a następnie przedstawione zostają najczęstsze metody oszustw internetowych wymierzonych w osoby starsze oraz przyczyny wzrostu tego typu przestępczości. Kluczową częścią pracy jest analiza prawnoporównawcza rozwiązań przyjętych w wybranych krajach. Na podstawie powyższych ustaleń, w zakończeniu podjęto próbę wskazania możliwych działań, które mogą przyczynić się do ograniczenia wzrostu skali oszustw wymierzonych w osoby starsze.

### **INTRODUCTION**

When we think about who should be particularly protected against various types of threats on the Internet, children come to mind first. There are specially designed applications and messengers for this group, and various types of control tools are available for their caregivers. This is also a group that is particularly protected by law. Over the last few years, the legal and policy framework to ensure even more effective child online safety has evolved considerably<sup>1</sup>.

<sup>1</sup> See e.g.: European strategy for a better Internet for kids (BIK+) - Compendium of legislation, <https://digital-strategy.ec.europa.eu/en/library/european-strategy-better-internet-kids-bik-compendium-legislation>. Particularly noteworthy are such international legal acts as: Audiovisual Media Services Directive (AVMSD, Directive (EU)



Meanwhile, the second group, which should receive equal attention, is neglected. In recent years, elderly people have been the most common victims of theft, burglary, and fraud online. The FBI estimates that in USA senior citizens only in 2020 lose more than \$3 billion to financial scams including romance scams and lottery and sweepstakes scams<sup>2</sup>. In this country, there was an 84% increase in elder fraud cases compared to 2022 and 2021 reports<sup>3</sup>. The number of cybercrimes against elderly people has also increased significantly in other countries. For example, in Poland one of the most common crimes committed against the elderly is fraud committed using the "grandson" and "policeman" methods. It is particularly severe because seniors often lose their entire life savings<sup>4</sup>. In Spain, one of the most common crimes in the digital world is fraud, which includes activities such as phishing, the malicious practice of impersonating another person or entity in order to obtain passwords, personal data, or access to bank accounts. As stated in the System of Crime Statistics (SEC), managed by the Ministry of Home Affairs, of all cybercrimes reported in 2019, 88% correspond to online fraud<sup>5</sup>. According to figures from 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 and Wales between April and September 2019 alone. Be it phishing emails, fake invoices, or phone tech support calls, scammers are attempting schemes against people who, in some cases, are the most vulnerable targets<sup>6</sup>. The examples above already illustrate the scale of the problem. However,

2018/1808), which obliges to protect minors from harmful content that may impair their physical, mental and moral development and illegal content and specified many rules to protect children from seeing illegal or harmful audiovisual content and inappropriate advertising on television and video-sharing platforms (like Youtube).

<sup>2</sup> Elder Fraud, <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/elder-fraud>. It's 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 elder people ages 70–79 did the same. The FBI speculates that this may be due to a lack of understanding of the reporting process. See more: A. O'driscoll, 30+ US cyber security and cybercrime statistics (2023) <https://www.comparitech.com/blog/information-security/us-cyber-crime-statistics/>

<sup>3</sup> M. Gill, Senior scam statistics 2023, <https://www.comparitech.com/identity-theft-protection/senior-scam-statistics/>

<sup>4</sup> Nearly 80 % of the victims are people over 70 years of age. See more: A. Rymaszewska, Seniorzy są łatwym celem oszustw w Internecie. Trzeba zadbać o ich edukację!, <https://www.dobreprogramy.pl/seniorzy-sa-latwym-celem-oszustw-w-internecie-trzeba-zadbac-o-ich-edukacje.6628728443115137a>

<sup>5</sup> Las estafas por internet representan más del 80% de los ciberdelitos, <https://www.newtral.es/estafas-internet-ciberdelitos/20210806/>

<sup>6</sup> D. Palmer, Cybersecurity: Why more needs to be done to help older people stay safe online, <https://www.zdnet.com/article/cybersecurity-why-more-needs-to-be-done-to-help-older-people-stay-safe-online/>

accurately measuring the scale of Internet fraud is beyond the cognitive capabilities of criminology<sup>7</sup>.

In most frauds perpetrators take advantage of gullibility and lack of vigilance, especially of elder and lonely people<sup>8</sup>. 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, e.g. regarding EU regulations 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 Eurostat, it is estimated that in 2020, 80% of the inhabitants of the European Union will use the Internet<sup>9</sup>. Among various age groups, the group aged 16-24 achieved the highest percentage, as much as 98%. However, statistics on elders (65-74 years old) show that 61% of elders in Europe use the Internet<sup>10</sup>.

Against this background the question arises: how should elderly people be protected by criminal law against various types of online fraud? Taking into account the diversity of

<sup>7</sup> The amount of information about the characteristics of criminals and victims of fraud on the Internet is particularly poor. 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. Also the main difficulty in the process of examining the scale of fraud against elder 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.

<sup>8</sup> See more about perpetrators and victims of online fraud: M. Siwicki, Charakterystyka sprawcy i ofiary "cyberoszustwa" [in:] Ambroziak T., Czwolek A., Gajewski S. [i in.] (ed.), Problemy bezpieczeństwa Europy i Azji, Toruń 2016, p. 450- 462.

<sup>9</sup> In 2020, 80% of adults in the EU used the internet daily, <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20211008-1>

<sup>10</sup> In this report Poland ranks 6th from the bottom. The only countries that fare worse are: Romania (40%), Portugal (39%), Greece (33%), Croatia (28%) and the Bulgaria (25%). On the other hand, in countries like Denmark, Luxemburg, Nederland, Sweden, the percentage of elder people using the Internet is over 90.

definitions of fraud, it is worth paying attention not only to the colloquial understanding of the concept of fraud, but also to the legal definitions. It is also important to pay attention to the modus operandi of the perpetrators of Internet fraud. This will help you to understand 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<sup>11</sup>. Of course, the decision to grant special protection to elderly people is always the responsibility of each country. But with the widely noticeable 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 make at least it more difficult for the perpetrators to choose the place of attack due to the 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 the contract, even if it concerns financial or material matters, should lead to criminal liability. The same applies to various types of problem and difficulties in settling mutual obligations in e-Commerce, which always involves a certain risk. Against this background, the second question arises: Should understanding of fraud also include conscious use of the gullibility, ignorance, or misunderstanding of elders?

## RESEARCH AND RESULTS

### I. The concept of fraud

In the colloquial understanding, it is usually assumed that fraud is an intentional, dishonest, false, deceptive violation of existing rules of social co-existence (e.g. violation of applicable rules of conduct in business transactions) undertaken in order to achieve undue advantage

---

<sup>11</sup> 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 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.

(positive value) by causing another person or persons to regulation unfavorable for them. The aim of manipulation will most often be to obtain a financial benefit for the perpetrator. However, it may also act to obtain another benefit (e.g. personal benefit, including increasing prestige, reputation, improving creditworthiness, etc., or various types of political benefits).

The dictionary emphasizes that the term fraud can be defined by referring to a qualifying feature that tries to mislead another person to obtain an undue advantage. As an example, we can point to the Polish dictionary, where fraud is defined as deliberately <sup>70</sup>misleading someone or taking advantage of someone else's mistake for your own benefit<sup>12</sup>. The term fraud is defined similarly in foreign-language dictionaries. For example, in Black's Law Dictionary, when defining fraud, it is noted that it is a general term for various behaviors that are the product of human ingenuity of an individual nature, the purpose of which is to gain an advantage over another person by creating a false impression or limiting the possibility of knowing the truth<sup>13</sup>. Fraud can include all kinds of tricks, mystifications, tricks, pretenses, and other unfair means by which another person is misled. <sup>44</sup>Such a broad approach means that in the dictionary mentioned above, fraud is divided into actual fraud, bank fraud, bankruptcy fraud, and criminal fraud and other fraudulent activities (fraudulent acts).

The advantage of the above definition is that it broadly covers behavior that may be classified as fraud, regardless of whether it resulted in property damage, personal injury, or any limitation of the injured party's ability to achieve his or her own goals. Based on the above understanding, authors such as <sup>41</sup>Joseph T. Wells, Nancy S. Bradford, Gilbert Geis, John D. Gill, W. Michael Kramer, James D. Ratley, and Jack Robertson divide fraud into:

- a) misrepresentation of material facts or false pretenses,
- b) concealment of material facts,
- c) Bribery
- d) Extortion
- e) Conflicts of interest.
- f) Forgery
- g) Embezzlement
- h) theft, and

<sup>12</sup> A. Bańkowski, *Etymologiczny Słownik Języka Polskiego*, t. II, Warszawa 2000, p. 457; E. Sobol, *Słownik języka polskiego*, Warszawa 2005, p. 623.

<sup>13</sup> ACFE, 2009 *Fraud Examiners Manual (International Edition)*, p. 2201, <http://thelawdictionary.org/fraud/>

i) Breach of fiduciary duty<sup>14</sup>.

Fraud is often classified as the so-called white-collar crime, i.e. crimes committed by a respected person or a person of significant social position who uses his reputation or position to commit a crime. Fraud is also treated as an important element of corporate crimes (Occupational Crime or Corporate Crime), i.e., crimes involving enrichment at the expense of the enterprise or for the benefit of the enterprise by persons employed in corporations<sup>15</sup>.

In practice, a broad definition of fraud may lead to a situation in which this term will have different, often diametrically opposed, meanings. Doubts as to its scope arise in particular in relation to various types of manipulation taking place in business activities. The same behavior of an entrepreneur operating on the market may be assessed by some as intellectual skill, by others as a tort, an offence giving rise to tort liability, and by others as an illegal act. This will include, among others: violations of various types of contractual provisions, guidelines regulating mutual business relations, internal operating instructions, work regulations, etc. In Poland, a certain problem in this respect was fraud in the sale of "wonderful" pots and kitchen utensils to elder people, in which the victims were misled as to the price and quality of the products. In the case of this type of activity, the perpetrators' activity was not initially assessed as fraud because elders had the opportunity to read what they signed. It was only later that attention was paid to the presentation of the goods sold and the rules of their purchase. During the resort shows, pensioners were forced to sign a number of documents, some of whom did not even know that they had signed loan agreements with very high interest rates<sup>16</sup>.

## II. 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

<sup>14</sup> J.T. Wells, N. S. Bradford, G. Geis, J. D. Gill, W. M. Kramer, J. D. Ratley, J. Robertson, *Fraud Examiners Manual (International Edition)*, Austin 2011, p. 670.

<sup>15</sup> Ch. Hlavica, U. Klapproth, *Tax Fraud & Forensic Accounting Umgang mit Wirtschaftskriminalität*, Wiesbaden 2011, p. 86-88.

<sup>16</sup> See e.g.: A. Jowša, Ruszył proces ws. oszustw przy sprzedaży "cudownych" garnków. Niemal 700 poszkodowanych, <https://www.bankier.pl/wiadomosc/Ruszy-proces-ws-oszustw-przy-sprzedazy-cudownych-garnkow-Niemal-700-poszkodowanych-8503140.html>



deterioration of elder adults (systemic decline in memory, processing speed, problem-solving ability, mathematical skills, linguistic ability and executive function)<sup>17</sup>, 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<sup>18</sup>. Naturally, the level of 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<sup>19</sup>. 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, for example, 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<sup>20</sup>. Research also found that the fraud techniques used by scammers are mainly focused on stimulating the victim's instincts<sup>21</sup>. 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

20

<sup>17</sup> A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Deci Support S.* 8, 51, p. 576–586.

<sup>18</sup> J. Shao, W. Du, T. Lin, X. Li, J. Li, H. Lei (2019). Credulity rather than general trust may increase vulnerability to fraud in older adults: a moderated mediation model. *J. Elder. Abuse Negl.* 31, p. 146–162.

<sup>19</sup> 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, *Front. Psychol.*, 05 September 2022, <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.912242/full>

<sup>20</sup> P. Fischer, S. E. Lea, K. M. Evans, (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *J. Community Appl. Soc. Psychol.* 43, 2060–2072.

<sup>21</sup> 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, *Front. Psychol.*, 05 September 2022, <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.912242/full>. In this text, the authors present a broader literature and make a detailed analysis.

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<sup>22</sup>.

In the so-called identity fraud, the perpetrator uses another person's personal information, without authorization, to commit to deceive or defraud other person for example by misleading the identity of the payment beneficiary<sup>23</sup>. 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, for example, 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 organisations.

<sup>22</sup> 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.

<sup>23</sup> United Kingdom, Cabinet Office (2002), *User Identity Fraud: A Study*, <https://www.ojp.gov/ncjrs/virtual-library/abstracts/identity-fraud-study>

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 website, banking and financial services, on-line stores, or on-line 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<sup>24</sup>.

Another form which is the simplest and at the same time most effective forms 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, for example, 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:

- a) failure to send the goods or failure to pay,
- b) sending a different product or one with a lower value than the agreed one,
- c) failure to disclose all relevant information about the product or terms of sale<sup>25</sup>.

Another, more complex, than the previous types of fraud, is the so-called investment fraud, in which the perpetrator, usually using e-mail, 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, for example, 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)<sup>26</sup>. Most often, it begins with establishing contact via email with a potential victim (formerly random, now

<sup>24</sup> See M. Siwicki, *Prawo karne*, p. 38-71. In this text, the authors present a broader literature and make a detailed analysis.

<sup>25</sup> Cf. e.g.: J. Clough, *Principles of cybercrime*, New York 2010, p. 183–199; C. Chin, *Cybercrime and Cyberfraud* [in:] *The Internet Encyclopedia*, vol. 1, H. Bidgoli (ed.), Hoboken 2004, p. 331-332.

<sup>26</sup> P. Bischoff, What is the Nigerian scam (419 scam) with examples, <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>

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, for example, 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 e-mail.

Equally often, the perpetrator may mislead about various phenomena and events. For example, a type of investment fraud called "pump and dump scam"<sup>27</sup> 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, for example as to the financial situation of a specific entrepreneur.

There are many factors that <sup>73</sup>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 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<sup>28</sup>.

It should also be mentioned that fraud on the Internet causes numerous forensic problems, in particular in the field of collecting evidence of the perpetrators' guilt. There are many factors that make it difficult to catch perpetrators of Internet fraud, including the frequent lack of material evidence, lack of understanding of the specific technology used by perpetrators

<sup>27</sup> See e.g.: M. La Morgia; A. Mei; F. Sassi; J. Stefa, Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations, <https://ieeexplore.ieee.org/document/9209660>; How Does a Pump-and-Dump Scam Work? <https://www.investopedia.com/ask/answers/05/061205.asp>

<sup>28</sup> 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. M. Siwicki, *Charakterystyka*, p. 450- 462.

to commit the crime, and the need to rely on the opinions of many specialists in the field of computer sciences. In addition to the above, prosecuting perpetrators of Internet fraud crimes is difficult due to anonymous nature of the Internet (fraudsters operate with relative impunity, making it harder to track them down and bring them to justice), jurisdictional issues (criminals often operate internationally, which can lead to jurisdictional issues), lack of evidence (perpetrators often try to cover their tracks), lack of victim cooperation (victims may be hesitant to report the crime or fear legal consequences), technological challenges (as technology advances, fraudsters find new ways to commit crimes, making it challenging for law enforcement to keep up) and complex legal procedures. Legal regulations may also vary depending on the jurisdiction, leading to confusion.

### III. 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 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<sup>29</sup>. However, there are significant differences in the regulations for fraud offences in individual countries, mainly in their detailed content, although individual types of prohibited acts show general similarities.

<sup>29</sup> The prototype of the crime of fraud was the Roman "stellionatus", which, based on the use of falsehood, violated property and other property rights. T. Oczkowski [in:] *Przestępstwa przeciwko mieniu i gospodarcze*, System Prawa Karnego tom 9, R. Zawłocki [ed.], Warszawa 2015, p. 117-120,



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, <sup>71</sup> according to Art. 209 of the Estonian Penal Code of 06/06/2001 (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<sup>30</sup>. In Bulgaria, according to Art. 209 of the Bulgarian Penal Code of May 1, 1968 ("Незаконни измами", Journal of Laws No. 24 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<sup>31</sup>. Similarly in Spain, according to Section 1, Article 248 of the Spanish Penal 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, and according to paragraph<sup>32</sup>.

In the German Penal Code (Strafgesetzbuch), where the offence of fraud (Betrug) is regulated in Chapter XXII, entitled "Fraud and abuse of trust" in Sect. 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)<sup>33</sup>. 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 Penal Code of 1889 (Journal of Laws 39/1889, as amended), fraud, according to Section 1 of Chapter 36 entitled 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<sup>34</sup>. The requirement to cause damage has also been adopted in other countries, such as Spain (art. 248), Italy (art. 640), Swiss (art. 146) and Poland (art. 286). But there are countries where fraud crime 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 (art. 326b) or Sweden (9 kap. 1 § Brottsbalken: "Bedrägeri"), where

<sup>61</sup> English translation: <https://w.riigiteataja.ee/en/eli/522012015002/consolide>

<sup>31</sup> English translation: <https://www.mlsp.government.bg/uploads/1/blgarsko-zakonodatelstvo/en/criminal-code.pdf>

<sup>32</sup> English translation: [https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal\\_Code\\_2016.pdf](https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf)

<sup>33</sup> English translation: [https://www.gesetze-im-internet.de/englisch\\_stgb/](https://www.gesetze-im-internet.de/englisch_stgb/)

<sup>34</sup> English translation: [https://www.finlex.fi/en/laki/kaannokset/1889/en18890039\\_19951010.pdf](https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_19951010.pdf)

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 the above-mentioned 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 Tatsachen), by concealment, 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 art. 146 of the Swiss Penal Code<sup>35</sup>. 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)<sup>36</sup>. 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 art. 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, 173)<sup>37</sup>. Also, under the Swedish Penal Code, which 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 (sec. 1). In other countries this additional feature is also introduced (art. 177 1 qualified form art. 122 § 6 of the Slovak Penal Code; art. 177 (1)

<sup>35</sup> English translation: <https://www.warnathgroup.com/wp-content/uploads/2017/11/Switzerland-Penal-Code-2017.pdf>

<sup>36</sup> English translation: [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](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)

<sup>37</sup> Also 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](https://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F126-IV-165%3Ade&lang=de&type=show_document)



of the Latvian Penal Code (use of bad faith, trust or by deceit<sup>38</sup>) and art. 190 Criminal Code of the Republic of Ukraine (deceit or breach of confidence)<sup>39</sup> and art. 248 the Spanish Penal 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 <sup>24</sup> 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 <sup>24</sup> 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, for example, immaturity) and of a temporary nature (when the cause is, for example, intoxication). For example, in France, according to Article 223-15-2 of the French Penal Code of 1992, "Escroquerie" is punishable to fraudulently abuse the recklessness or weakness of a minor or the special sensitivity of another person <sup>77</sup> 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 techniques fraudulently 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 penal code according to art. 209 (2) The (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 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). <sup>2</sup> It is also worth paying attention to the solutions adopted in Slovakia, where the qualified type of fraud, punishable by imprisonment of 3 to 10 years, is defined in Art. 3 of the Code. 221 (Slovak Podvod)<sup>40</sup>. The qualifying features in this case are:

<sup>38</sup> English translation: <https://www.at.gov.lv/en/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/klasifikators-pec-lietu-kategorijam/latvijas-kriminalkodekss>

<sup>39</sup> 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](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)

<sup>40</sup> English translation: <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/>

- a) significant damage resulting from the crime committed (pursuant to Article 125, significant damage is a value that is at least 100 times EUR),
- b) committing a crime with a special motivation,
- c) committing a crime in a particular way, and
- d) committing a crime to the detriment of the protected person.

The mark of committing a crime in a specific way was defined in the art. 138 of the Slovak Penal 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 art. 139 of the Slovak Penal 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.

The legislation of European countries also varies in terms of the severity of penalization. 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 5,000 euros, it is punishable by imprisonment for up to 3 years, and if the damage amounted to more than 300,000 euros, imprisonment from one 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 three 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 five years. In Bulgaria, fraud is punishable by one to six years of deprivation of liberty. In Poland fraud is punishable to 8 years of deprivation of liberty<sup>41</sup>.

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 tort of deceit. Although the precise

<sup>41</sup> See M. Siwicki, Prawo karne, p. 38-71.

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

a) 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,

b) 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. Heathon 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"<sup>42</sup>.

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<sup>43</sup>.

In the U.S. federal statute governing fraud at 18 U.S.C. 1341<sup>44</sup>, it is assumed that, in the case of fraud crime, it is necessary to prove the existence of five elements:

1) false presentation of an important fact by the perpetrator,

<sup>42</sup> R. Heathon, *Criminal Law, Textbook*, Oxford 2006, p. 327

<sup>43</sup> M. Šepec, *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis*, *International Journal of Cyber Criminology (IJCC)*, July – December 2012, Vol 6 (2), p. 984–1000.

<sup>44</sup> US Code – Code of Laws in the United States (A comprehensive Code of the United States) online: <http://www.law.cornell.edu/uscode/>

- 2) awareness on the part of the perpetrator that such facts are untrue,
- 3) the intention to defraud the alleged victim (e.g. deprive him of some entitlement),
- 4) damage to the alleged victim as a result of the perpetrator's actions,
- 5) acts to obtain money or property.

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:

- 1) false representation (section 2),
- 2) fraud by failing to disclose information (section 3),
- 3) fraud by abuse of position - (section 4).

The first type of fraud requires the following:

- a) knowingly presenting false or misleading facts, information, or law;
- b) 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,

58

the case of *Derry v Peek* (1889) LR 14 App Cas 337<sup>45</sup> and *Hedley Byrne & Co Ltd v Heller & Partners Ltd* (1964) AC 465<sup>46</sup> are typical in this respect.

28

Similarly, to the above-mentioned Switzerland, in Ireland, the crime 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 judgement 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.

## DISCUSSION AND CONCLUSIONS

76

In recent years, we have seen that the number of online frauds has increased dramatically and shows no signs of abating. Over time, perpetrators began to use increasingly complex methods and techniques, starting with phishing, through the creation of professional software and hardware tools, ending with the use of the so-called enterprises that provide protection to cybercriminals and the creation of associations which diversify the activities of participants within the functional division of labor.

The increase in the number of frauds on the Internet not only increases the risk of business activity, negatively affects the sense of security, and increases transaction costs, but also negatively affects interpersonal relationships, contributing to the reduction of people's trust in each other. Another problem that may be encountered in the case of fraud committed on the Internet is the lack of a clear and common definition of what is meant by fraud. For obvious reasons, this may complicate efforts to combat this phenomenon, mainly due to its global and cross-border nature. Difficulties may arise, among others: in the field of research and measurement of crime, development of common policy, public education, assistance to victims, or the development of common methods and techniques of prevention. Although standard

<sup>45</sup> <http://www.e-lawresources.co.uk/Derry-v-Peek.php>

<sup>46</sup> <http://www.bailii.org/cgi-bin/markup.cgi?doc=/uk/cases/UKHL/1963/4.html>

definitions can be used to optimize countermeasure strategies, they are by no means necessary to solve a problem. The existence of many definitions in the international arena may, in practice, also lead to the same problem being solved in different ways, at the same time providing an indication of a possible path of development for others.

The above comments of a comparative law nature make it clear that the concept of fraud covers various behaviors of perpetrators, which may be tolerated or combated with criminal law measures under individual legal systems. Typically, in the case of fraud, unlike theft and misappropriation, which always lead to financial gain for the perpetrator (or someone else), the benefit does not have to occur. In comparative law, especially in the countries of the Anglo-Saxon system, the voluntary disposition of property by the defrauded person to the perpetrator is not always a qualifying feature. It is not always irrelevant to the existence of the crime of fraud whether the injured party could have detected the error even with the slightest care. The subject of the assessment may also be the Un criticality and gullibility of the injured party. A common feature is that the perpetrators consciously present false or misleading facts to a specific person (creating a false impression) and act in order to obtain unlawful financial gain for themselves or another person (the perpetrator's act is directed against property).

These few examples already make it clear that there are significant differences in approaches to protecting against fraud. It is much easier to protect older people in countries where assessments of diligence, the purpose of the perpetrator's action, or the specific method of his action are not required. If we want to stop the increase in fraud crimes against the elderly, it is worth paying attention to the above-mentioned solutions that provide aggravated crime by taking advantage of specific weaknesses of other people.

Given that there are millions of scam victims each year, it is urgently necessary to identify what factors make older people more vulnerable to scams and, more importantly, what preventive measures can be used to alleviate this problem. There is a growing need to develop theoretical frameworks that incorporate cognitive abilities, neurological insights, and personality research that can advance understanding susceptibility to fraud among elder people. Because little is known about how to reduce Internet fraud, there is an urgent need to conduct research in this area that will make it possible to develop decision aids and other tools to reduce this phenomenon. Although many sources on the Internet offer valuable advice, many elderly people do not follow it. Given the complex nature of the problem, closer collaborations among

<sup>3</sup> researchers in different disciplines (e.g., computer scientists and psychologists) are likely to be fruitful. It also seems justified to introduce changes to the applicable legislation to counteract fraud on the Internet. It is worth considering not only its unification, at least within the European Union, but also adopting solutions for the special protection of elderly people.

Proper counteracting fraud on the Internet against elderly people requires limiting the physical possibility of committing a crime by using various types of hardware and software security measures and striving to deprive perpetrators of the tools (technical and software) used to commit crimes. It is equally important to place greater emphasis on increasing the risk of being caught and convicted for the crimes committed by the perpetrator. Achieving the latter goal requires a detailed analysis of specific forms of crime, including collecting data on its nature and dimensions. In the case of fraud against elderly people, it seems reasonable to pay attention primarily to the conditions that enable or facilitate the commission of this crime and, consequently, to systematically limit them. Such activities should primarily focus on creating appropriate supervision and control systems, defining rules for access to computer systems, and detailed monitoring and identification of users. The purpose of this last action should be primarily to prevent the perpetrators from masking their identity and location. At the same time, as in the case of all crimes on the Internet, the fight against fraud should be intensified not only by undertaking international cooperation, but also by educating and raising public awareness. Effective counteracting fraud on the Internet cannot be based only on actions taken by the state, but should be supported - through cooperation with internet service providers and end users (e.g. development of self-control).

## REFERENCES

### Literature

- <sup>60</sup> Bańkowski A., *Etymologiczny Słownik Języka Polskiego*, t. II, Warszawa 2000
- Chin C., *Cybercrime and Cyberfraud* [in:] *The Internet Encyclopedia*, vol. 1, H. Bidgoli [ed.], Hoboken 2004
- <sup>18</sup> Bischoff P., What is the Nigerian scam (419 scam) with examples, <https://www.comparitech.com/identity-theft-protection/nigerian-scam/>
- Clough J., *Principles of cybercrime*, New York 2010



- 1 Fischer, P., Lea, S. E., and Evans, K. M. (2013). *Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance*. J. Community Appl. Soc. Psychol. 43
- 25 Gill M., Senior scam statistics 2023, <https://www.comparitech.com/identity-theft-protection/senior-scam-statistics/>
- 42 Heathon R., *Criminal Law, Textbook* Oxford 2006
- 42 Hlavica Ch., U. Klapproth, *Tax Fraud & Forensic Accounting Umgang mit Wirtschaftskriminalität*, Wiesbaden 2011
- 14 Jowsa A., Ruszył proces ws. oszustw przy sprzedaży "cudownych" garnków. Niemal 700 poszkodowanych, <https://www.bankier.pl/wiadomosc/Ruszyl-proces-ws-oszustw-przy-sprzedazy-cudownych-garnkow-Niemal-700-poszkodowanych-8503140.html>
- 23 Morgia M. La; Mei A.; Sassi F.; Stefa J., *Pump and Dumps in the Bitcoin Era: Real Time Detection of Cryptocurrency Market Manipulations*, <https://ieeexplore.ieee.org/document/9209660>
- 44 Palmer D., *Cybersecurity: Why more needs to be done to help older people stay safe online*, <https://www.zdnet.com/article/cybersecurity-why-more-needs-to-be-done-to-help-older-people-stay-safe-online/>
- 13 Rymśza A., *Seniorzy są łatwym celem oszustw w Internecie. Trzeba zadbać o ich edukację!*, <https://www.dobreprogramy.pl/seniorzy-sa-latwym-celem-oszustw-w-internecie-trzeba-zadbać-o-ich-edukację.6628728443115137a>
- 13 Shang Y., Wu Z., Du X., Jiang Y., Mal B., Chi M., *The psychology of internet fraud victimization of older adults: A systematic review*, Front. Psychol., 05 September 2022, <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.912242/full>
- 13 Shao J., Du W., Lin T., Li X., Li J., Lei H. (2019). *Credulity rather than general trust may increase vulnerability to fraud in older adults: a moderated mediation model*. J. Elder. Abuse Negl. 31
- 17 Siwicki M., *Charakterystyka sprawcy i ofiary "cyberoszustwa"* [in:] Ambroziak T., Czwolek Gajewski S. [i in.] (ed.), *Problemy bezpieczeństwa Europy i Azji*, Toruń 2016
- 17 Siwicki M., *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu internetowym oraz bankowości elektronicznej*, Toruń 2018
- 16 Pol E., *Słownik języka polskiego*, Warszawa 2005
- 35 Sepec M., *Slovenian Criminal Code and Modern Criminal Law Approach to Computer-related Fraud: A Comparative Legal Analysis*, International Journal of Cyber Criminology (IJCC), July – December 2012, Vol 6 (2)
- 35 O'driscoll A., 30+ US cyber security and cybercrime statistics (2023) <https://www.comparitech.com/blog/information-security/us-cyber-crime-statistics/>
- 1 Oczkowski T. (in:) *Przestępstwa przeciwko mieniu i gospodarcze*, System Prawa Karnego tom 1 Zawłocki R. (ed.), Warszawa 2015
- 33 Vishwanath A., Herath T., Chen R., Wang J., Rao H. R. (2011). *Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model*. Deci Support Syst. 51
- Wells J.T., Bradford N. S., Geis G., Gill J. D., Kramer W. M., Ratley J. D., Robertson J., *Fraud Examiners Manual (International Edition)*, Austin 2011



- Criminal Code of Germany** (2018). BGBl. 2024 I Nr. 109. Retrieved from: <https://www.gesetze-im-internet.de/stgb/>
- Criminal Code of Bulgaria** (2017). SG No. 85/24.10.2017. Retrieved from: <https://www.misp.government.bg/uploads/1/blgarsko-zakonodatelstvo/en/criminal-code.pdf>
- Criminal Code of Slovakia** (2019). 474/2019 Coll. Retrieved from: <https://legislationline.org/Slovakia>
- Criminal Code of Spain** (2024). Organic Law 10/1995, of November 23, 33987-34058. Retrieved from: [https://www.boe.es/biblioteca\\_juridica/codigos/codigo.php?id=038](https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=038)
- Criminal Code of Estonia** (2001). RT I 2001, 61, 364. Retrieved from: <https://www.riigiteataja.ee/en/eli/522012015002/consolide>
- Criminal Code of Finland** (2022). Retrieved from: [https://finlex.fi/en/iki/kaannokset/1889/en18890039\\_19951010.pdf](https://finlex.fi/en/iki/kaannokset/1889/en18890039_19951010.pdf)
- Criminal Code of France** (2024). Retrieved from: [https://www.legifrance.gouv.fr/codes/texte\\_lc/LEGITEXT000006070729/?isSuggest=true](https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070729/?isSuggest=true)
- Criminal Code of Italy** (2018). Retrieved from: <https://legislationline.org/taxonomy/term/23690>
- Criminal Code of the Republic of Ukraine** (2001). Retrieved from: <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>
- Criminal Code of the Netherlands** (2012). Retrieved from: [https://legislationline.org/sites/default/files/documents/f3/Netherlands\\_CC\\_am2012\\_en.pdf](https://legislationline.org/sites/default/files/documents/f3/Netherlands_CC_am2012_en.pdf)
- Criminal Code of Latvia** (2023). Retrieved from: <https://www.at.gov.lv/en/tiesu-prakse/judikaturas-nolemumu-arhivs/kriminallietu-departaments/klasifikators-pec-lietu-kategorijam/latvijas-kriminalkodekss>
- Criminal Code of Poland** (2024). Dz. U. z 2024 r. poz. 17. Retrieved from: <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970880553/U/D19970553Lj.pdf>
- Criminal Code of Switzerland** (2020). StGB, SR 311.0. Retrieved from: <https://www.rhf.admin.ch/rhf/de/home/strafrecht/rechtsgrundlagen/national/sr-311-0.html>
- Criminal Code of Sweden** (2020). SFS 1962:700 Brottsbalken. Retrieved from: <https://www.government.se/government-policy/judicial-system/the-swedish-criminal-code/>

# Protecting elderly people from online fraud. Comparative Law Aspects (iThenticate Similarity Report)

## ORIGINALITY REPORT

25%

SIMILARITY INDEX

## PRIMARY SOURCES

|   |                                                                                                                                                                                                         |                |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 1 | <a href="http://www.frontiersin.org">www.frontiersin.org</a><br>Internet                                                                                                                                | 300 words — 3% |
| 2 | <a href="http://sls-journal.com.ua">sls-journal.com.ua</a><br>Internet                                                                                                                                  | 142 words — 1% |
| 3 | Yaniv Hanoch, Stacey Wood. "The Scams Among Us: Who Falls Prey and Why", Current Directions in Psychological Science, 2021<br>Crossref                                                                  | 122 words — 1% |
| 4 | <a href="http://www.zdnet.com">www.zdnet.com</a><br>Internet                                                                                                                                            | 98 words — 1%  |
| 5 | <a href="http://www.cybercrimejournal.com">www.cybercrimejournal.com</a><br>Internet                                                                                                                    | 94 words — 1%  |
| 6 | <a href="http://acts2.oireachtas.ie">acts2.oireachtas.ie</a><br>Internet                                                                                                                                | 85 words — 1%  |
| 7 | <a href="http://tmp.comparitech.com">tmp.comparitech.com</a><br>Internet                                                                                                                                | 81 words — 1%  |
| 8 | Hongliang Chen, Yunsha Pu, David Atkin. "Migration stress, risky Internet uses, and scam victimization: An empirical study among Chinese migrant workers", Telematics and Informatics, 2023<br>Crossref | 64 words — 1%  |

|    |                                                                                                                                                                                                       |                  |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 9  | <a href="http://nli.gov.mn">nli.gov.mn</a><br>Internet                                                                                                                                                | 60 words — 1 %   |
| 10 | <a href="http://dspace.tltsu.ru">dspace.tltsu.ru</a><br>Internet                                                                                                                                      | 51 words — 1 %   |
| 11 | <a href="http://www.brennerbasisdemokratie.eu">www.brennerbasisdemokratie.eu</a><br>Internet                                                                                                          | 50 words — 1 %   |
| 12 | <a href="http://www.bankier.pl">www.bankier.pl</a><br>Internet                                                                                                                                        | 48 words — < 1 % |
| 13 | <a href="http://www.dobreprogramy.pl">www.dobreprogramy.pl</a><br>Internet                                                                                                                            | 48 words — < 1 % |
| 14 | <a href="http://www.mdpi.com">www.mdpi.com</a><br>Internet                                                                                                                                            | 48 words — < 1 % |
| 15 | <a href="http://www.hindawi.com">www.hindawi.com</a><br>Internet                                                                                                                                      | 46 words — < 1 % |
| 16 | <a href="http://pdfs.semanticscholar.org">pdfs.semanticscholar.org</a><br>Internet                                                                                                                    | 44 words — < 1 % |
| 17 | <a href="http://bip.uwb.edu.pl">bip.uwb.edu.pl</a><br>Internet                                                                                                                                        | 40 words — < 1 % |
| 18 | <a href="http://quieora.ink">quieora.ink</a><br>Internet                                                                                                                                              | 36 words — < 1 % |
| 19 | <a href="http://www.neimanepartners.com">www.neimanepartners.com</a><br>Internet                                                                                                                      | 34 words — < 1 % |
| 20 | Edwin D. Frauenstein, Stephen V. Flowerday.<br>"Social network phishing: Becoming habituated to clicks and ignorant to threats?", 2016 Information Security for South Africa (ISSA), 2016<br>Crossref | 33 words — < 1 % |

|    |                                                                                                         |                  |
|----|---------------------------------------------------------------------------------------------------------|------------------|
| 21 | <a href="http://eur-lex.europa.eu">eur-lex.europa.eu</a><br>Internet                                    | 32 words — < 1 % |
| 22 | <a href="http://lawscience.com.ua">lawscience.com.ua</a><br>Internet                                    | 32 words — < 1 % |
| 23 | "Artificial Intelligence and International Human Rights Law", Edward Elgar Publishing, 2024<br>Crossref | 30 words — < 1 % |
| 24 | Syed R. Ahmed. "Preventing Identity Crime: Identity Theft and Identity Fraud", Brill, 2020<br>Crossref  | 30 words — < 1 % |
| 25 | <a href="http://www.anserpress.org">www.anserpress.org</a><br>Internet                                  | 30 words — < 1 % |
| 26 | <a href="http://delibra.bg.polsl.pl">delibra.bg.polsl.pl</a><br>Internet                                | 27 words — < 1 % |
| 27 | Mike Molan. "Cases and Materials on Criminal Law", Routledge-Cavendish, 2009<br>Publications            | 25 words — < 1 % |
| 28 | <a href="http://studentshare.org">studentshare.org</a><br>Internet                                      | 25 words — < 1 % |
| 29 | <a href="http://dolgozattar.uni-bge.hu">dolgozattar.uni-bge.hu</a><br>Internet                          | 24 words — < 1 % |
| 30 | <a href="http://www.rfmlr.com">www.rfmlr.com</a><br>Internet                                            | 24 words — < 1 % |
| 31 | <a href="http://wwwusers.di.uniroma1.it">wwwusers.di.uniroma1.it</a><br>Internet                        | 24 words — < 1 % |
| 32 | <a href="http://en.wikipedia.org">en.wikipedia.org</a><br>Internet                                      | 23 words — < 1 % |

|    |                                                                                                                                                                                                   |                  |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 33 | eprints.umg.ac.id<br>Internet                                                                                                                                                                     | 22 words — < 1 % |
| 34 | medf.kg.ac.rs<br>Internet                                                                                                                                                                         | 22 words — < 1 % |
| 35 | www.dbxuk.com<br>Internet                                                                                                                                                                         | 22 words — < 1 % |
| 36 | api.perma.cc<br>Internet                                                                                                                                                                          | 21 words — < 1 % |
| 37 | cks.univnt.ro<br>Internet                                                                                                                                                                         | 21 words — < 1 % |
| 38 | Oleksandr Sotula. "The Violation of the Laws of Armed Conflict in the Ukrainian and Polish Dimension: The Criminal Law Discourse", Acta Universitatis Lodzensis. Folia Iuridica, 2024<br>Crossref | 20 words — < 1 % |
| 39 | hornellsun.com<br>Internet                                                                                                                                                                        | 20 words — < 1 % |
| 40 | Paul Barnes. "Stock Market Efficiency, Insider Dealing and Market Abuse", Gower, 2016<br>Publications                                                                                             | 19 words — < 1 % |
| 41 | www.tandfonline.com<br>Internet                                                                                                                                                                   | 19 words — < 1 % |
| 42 | www.alexandria.unisg.ch<br>Internet                                                                                                                                                               | 18 words — < 1 % |
| 43 | cotopaxi-colorado.com<br>Internet                                                                                                                                                                 | 17 words — < 1 % |
| 44 | epdf.pub<br>Internet                                                                                                                                                                              | 17 words — < 1 % |

|    |                                                                                         |                  |
|----|-----------------------------------------------------------------------------------------|------------------|
| 45 | <a href="https://www.scribd.com">www.scribd.com</a><br>Internet                         | 17 words — < 1 % |
| 46 | "The Asian Yearbook of Human Rights and Humanitarian Law", Brill, 2023<br>Crossref      | 16 words — < 1 % |
| 47 | <a href="https://myjms.mohe.gov.my">myjms.mohe.gov.my</a><br>Internet                   | 16 words — < 1 % |
| 48 | <a href="https://insideparadeplatz.ch">insideparadeplatz.ch</a><br>Internet             | 15 words — < 1 % |
| 49 | "The Handbook of Comparative Criminal Law", Walter de Gruyter GmbH, 2010<br>Crossref    | 14 words — < 1 % |
| 50 | <a href="https://drept.hyperion.ro">drept.hyperion.ro</a><br>Internet                   | 14 words — < 1 % |
| 51 | <a href="https://lawjournal.com.ua">lawjournal.com.ua</a><br>Internet                   | 14 words — < 1 % |
| 52 | <a href="https://kuza.tibet.org">kuza.tibet.org</a><br>Internet                         | 13 words — < 1 % |
| 53 | <a href="https://guies.uab.cat">guies.uab.cat</a><br>Internet                           | 12 words — < 1 % |
| 54 | <a href="https://repositori.tecnocampus.cat">repositori.tecnocampus.cat</a><br>Internet | 12 words — < 1 % |
| 55 | <a href="https://coffers.eu">coffers.eu</a><br>Internet                                 | 11 words — < 1 % |
| 56 | <a href="https://iris.unitn.it">iris.unitn.it</a><br>Internet                           | 11 words — < 1 % |

|    |                                                                                                                                                           |                  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| 57 | revista.unap.ro<br>Internet                                                                                                                               | 11 words — < 1 % |
| 58 | www.coursehero.com<br>Internet                                                                                                                            | 11 words — < 1 % |
| 59 | crimesciencejournal.biomedcentral.com<br>Internet                                                                                                         | 10 words — < 1 % |
| 60 | dspace.uni.lodz.pl<br>Internet                                                                                                                            | 10 words — < 1 % |
| 61 | library.oapen.org<br>Internet                                                                                                                             | 10 words — < 1 % |
| 62 | wnus.edu.pl<br>Internet                                                                                                                                   | 10 words — < 1 % |
| 63 | blog.ipleaders.in<br>Internet                                                                                                                             | 9 words — < 1 %  |
| 64 | environmentalscience.com.ua<br>Internet                                                                                                                   | 9 words — < 1 %  |
| 65 | opus.bibliothek.uni-augsburg.de<br>Internet                                                                                                               | 9 words — < 1 %  |
| 66 | Ann Wolbert Burgess, Robert R. Hazelwood.<br>"Practical Aspects of Rape Investigation - A<br>Multidisciplinary Approach", CRC Press, 2025<br>Publications | 8 words — < 1 %  |
| 67 | Chris Bevan. "The Routledge Handbook of Global<br>Perspectives on Homelessness, Law & Policy",<br>Routledge, 2024<br>Publications                         | 8 words — < 1 %  |
| 68 | Joycelyn Pollock. "Criminal Law", Routledge, 2019<br>Publications                                                                                         | 8 words — < 1 %  |

|    |                                                                                                                                                                           |                 |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| 69 | PNLD, Police National Legal Database, Ozin QC, Paul. "Blackstone's Police Operational Handbook 2023", Blackstone's Police Operational Handbook 2023, 2022<br>Publications | 8 words — < 1 % |
| 70 | blr.flaw.uniba.sk<br>Internet                                                                                                                                             | 8 words — < 1 % |
| 71 | dspace.nplg.gov.ge<br>Internet                                                                                                                                            | 8 words — < 1 % |
| 72 | researchspace.ukzn.ac.za<br>Internet                                                                                                                                      | 8 words — < 1 % |
| 73 | www.dbc.wroc.pl<br>Internet                                                                                                                                               | 8 words — < 1 % |
| 74 | www.researchgate.net<br>Internet                                                                                                                                          | 8 words — < 1 % |
| 75 | www.ukessays.com<br>Internet                                                                                                                                              | 8 words — < 1 % |
| 76 | Emma L. Briant, Vian Bakir. "Routledge Handbook of the Influence Industry", Routledge, 2024<br>Publications                                                               | 7 words — < 1 % |
| 77 | Ellen Pinkos Cobb. "International Workplace Sexual Harassment Laws and Developments for the Multinational Employer", Routledge, 2019<br>Publications                      | 6 words — < 1 % |
| 78 | Tickner Peter. "Fraud and Corruption in Public Services", Routledge, 2017<br>Publications                                                                                 | 6 words — < 1 % |

EXCLUDE QUOTES            OFF  
EXCLUDE BIBLIOGRAPHY   OFF

EXCLUDE SOURCES        OFF  
EXCLUDE MATCHES        OFF