CZU: 04.056.53:657.1(478)

SECURITATEA INFORMAȚIEI FINANCIAR-CONTABILE ÎN CONTEXTUL EVOLUȚIEI DIGITALE

Conf. univ. dr. Silvia ZAHARCO, USM
silvia.zaharco@usm.md
ORCID: 0000-0003-0988-9152
DOI: https://doi.org/10.53486/econ.2023.124.070

În *prezentul studiu se analizează modalitățile de scurgere a informațiilor confidențiale, circumstanțele de prezentare legală a informației aferente activității entităților, precum și responsabilitățile aferente divulgării datelor cu caracter confidențial. Scopul lucrării este elucidarea necesității de a securiza informațiile financiar-contabile și de a spori conștientizarea profesioniștilor contabili în ceea ce privește apariția riscurilor generate de digitalizarea proceselor economice. Metodologia cercetării s-a axat pe utilizarea metodelor tradiționale, în special analiza în dinamică și cea structurală a fenomenului cercetat. Ca urmare a observațiilor efectuate, putem menționa că securizarea informației financiar-contabile asigură confidențialitatea acesteia, respectiv previne cauzarea unor prejudicii financiare sau de altă natură. În Republica Moldova nu există un raport sau o bază de date cu acces deschis, care ar reflecta situația aferentă securizării informației financiar-contabile pe plan național, prin urmare, în lucrare au fost analizate datele înregistrate la nivel mondial.*

Cuvinte-cheie: *confidențialitate, divulgare, fraudă, măsuri de securitate, scurgere de informații.*

JEL: G14, K13, M49.

Introducere

Trăim într-o eră digitalizată, în care majoritatea interacțiunilor noastre se desfășoară în mediul virtual, iar impunerea restricțiilor, privind contactul fizic în pandemia COVID-19, a întărit aceste tendințe, accelerând transformarea digitală a societății.

Transformarea digitală a activităților de afaceri este una dintre cele mai importante ten-

UDC: 04.056.53:657.1(478)

SECURITY OF FINANCIAL AND ACCOUNTING INFORMATION IN THE CONTEXT OF DIGITAL EVOLUTION

Assoc. Prof. PhD Silvia ZAHARCO, MSU
silvia.zaharco@usm.md
ORCID: 0000-0003-0988-9152
DOI: https://doi.org/10.53486/econ.2023.124.070

This study analyses the ways of leaking confidential information, the circumstances of legal presentation of the information related to the activity of entities, as well as the responsibilities related to the disclosure of confidential data. The purpose of this article is to elucidate the need to secure financial and accounting information and increase the awareness of accounting professionals regarding the emergence of risks generated by the digitalization of economic processes. The research methodology focused on the use of traditional methods, especially the dynamic and structural analysis of the researched phenomenon. As a result of the observations made, we can mention that securing the financial and accounting information ensures its confidentiality, respectively prevents causing financial or other damages. There is no report or database in the Republic of Moldova with open access that would reflect the situation related to the securing of financial and accounting information, therefore, in the paper the data at the world level were reflected.

Keywords: *confidentiality, disclosure, fraud, security measures, information leakage.*

JEL: G14, K13, M49.

Introduction

We live in a digitized age, where most of our interactions take place in the digital environment, and the restrictions on physical contact that were imposed during the COVID-19 pandemic has reinforced these trends, accelerating the digital transformation of the society.

Digital transformation of business activities is one of the most important trends, as it shapes the complex process how entities enable and apply innovations. Digitization involves the

dințe, deoarece modelează procesul complex în care entitățile activează și aplică inovațiile. Digitalizarea implică integrarea tehnologiei digitale în diverse domenii ale afacerii, schimbând substanțial modul de funcționare a unei entități. Amplificarea procesului de digitalizare este urmată de sporirea competitivității și dezvoltării tehnologiilor informaționale [10].

Evoluția tehnologiilor digitale a creat importante oportunități pentru consolidarea unor societăți prospere din punct de vedere economic. În același timp, au apărut mai multe amenințări periculoase la adresa securității datelor (cum ar fi: încălcarea confidențialității, pârtinirea algoritmică, cauzată de date necorespunzătoare, volatilitatea pieței etc.) [7, p. 4].

Cele mai dificil de identificat sunt amenințările la adresa domeniului economic, acesta însumând o gamă largă de entități. Riscurile de natură economică sunt mai greu de recunoscut, deoarece multe din manifestările lor aparțin dezechilibrelor economice uzuale și nu sunt orientate în mod direct împotriva statului. În același timp, entitățile fac parte din structura statului și constituie fundamentul acestuia [5, p. 8].

În literatura de specialitate există multe studii care tratează problematica securității informaționale, însă s-a acordat mai puțină atenție argumentelor care ar justifica necesitatea de securizare a informațiilor financiar-contabile și ar demonstra cum profesioniștii contabili contribuie la scăderea sau la creșterea riscului generat de digitalizarea proceselor [14].

Obiectivul lucrării este de a cerceta volumul scurgerilor de informații la nivel mondial, cauzele acestor scurgeri și măsurile pe care profesioniștii contabili trebuie să le aplice în scopul protejării datelor entităților sau clienților pentru care lucrează și ale organismelor profesionale.

Metodologia cercetării

Baza informațională a cercetării este reprezentată de diverse lucrări din domeniu, în special Raportul de investigare privind scurgerile de informații confidențiale (InfoWatch Expert) și Raportul privind situația amenințărilor scurgerilor de informații (ENISA). De asemenea, au fost puse în practică *diverse metode de cercetare*, cum ar fi: *analiza sistemică, analiza în dinamică* și cea *structurală, metoda observației și a com-*

integration of digital technology in various areas of business, fundamentally changing the way an entity operates. The amplification of the digitization process is followed by the increase in competitiveness and the development of information technologies [10].

The evolution of digital technologies has created important opportunities for the consolidation of economically prosperous societies. At the same time, several dangerous threats to data security (such as privacy breach, algorithmic bias caused by bad data, market volatility, etc.) have emerged [7, p. 4].

The most difficult to identify are the threats to the economic field, being represented by a wide range of entities. Economic threats are more difficult to identify, since many of their manifestations belong to natural economic imbalances and are not directly directed against the state. At the same time, the entities are part of the state structure and constitute its foundation [5, p. 8].

In the literature, there are multiple studies dealing with the issue of information security, but less attention has been paid to the level of understanding the need to secure financial and accounting information and how accounting professionals contribute to decreasing or increasing the risk generated by the digitization of processes [14].

The objective of this paper is to investigate the volume of information leakages worldwide, the causes of these leakages and the measures that professional accountants must apply in order to protect the data of the entities or clients they work for and of professional bodies.

Research methodology

The informational basis of the article was constituted by various works in the field, in particular, the Investigation Report on the leakage of confidential information (InfoWatch Expert) and the Report on the situation of information leakage threats (ENISA). *Various research methods* were used for its processing, such as: *systemic analysis, dynamic and structural analysis, observation method, comparison method*. The analysis of the legislation in force was also used, in order to identify the punishments applicable to those who make confidential information public.

parației. S-a apelat și la analiza legislației în vigoare, pentru a identifica pedepsele aplicabile celor care fac publice informațiile confidențiale.

Rezultate și discuții

Unul dintre principiile fundamentale ce reglementează activitatea profesionistului contabil este confidențialitatea. Acesta prevede respectarea confidențialității informațiilor dobândite ca urmare a relațiilor profesionale, de afaceri și, prin urmare, nedivulgarea acestora către părți terțe. Respectiv, se interzice folosirea informației confidențiale de către profesionistul contabil în avantajul său sau al altor părți terțe, cu excepția cazului în care există un drept sau o obligație legală, sau profesională, de a dezvălui aceste informații [11, pp. 21-22].

Astfel, principiul confidențialității impune abstinența de la:

a) dezvăluirea informațiilor confidențiale în afara entității angajatoare, cu excepția cazului în care există o obligație legală sau profesională de a face publice acele informații;
b) folosirea datelor și informațiilor confidențiale obținute în cadrul relațiilor profesionale în interesul personal sau al unor părți terțe.

Angajamentul de respectare a principiului confidențialității se menține și după încheierea relației dintre un profesionist contabil și angajator/client. În cazul schimbării locului de muncă sau obținerii unui nou client, profesionistul contabil nu trebuie să folosească sau să prezinte informațiile confidențiale obținute dintr-o relație profesională sau de afaceri.

Totuși, în anumite circumstanțe (figura 1), informațiile confidențiale pot fi prezentate, luând în considerare următorii factori:

- gradul de afectare sau prejudiciere a intereselor tuturor părților, inclusiv a părților terțe;
- relevanța informațiilor și fundamentarea acestora, în măsura în care este posibil;
- modalitatea de comunicare preconizată și interlocutorul.

Results and discussions

One of the fundamental principles governing the activity of the professional accountant is confidentiality. It provides for respecting the confidentiality of information acquired as a result of professional and business relationships and, therefore, not disclosing this information to third parties or using the confidential information for its personal advantage or that of other third parties, unless there is a legal right or obligation or professional to disclose this information [11, pp. 21-22].

Thus, the principle of confidentiality requires avoiding such actions like:

a) disclosure of confidential information outside the employing entity, unless there is a legal or professional obligation to make that information public;
b) using confidential data and information acquired as a result of professional relationships for personal benefit or for the benefit of third parties.

The commitment to respect the principle of confidentiality is maintained even after the end of the relationship between a professional accountant and employer or client. When changing jobs or acquiring a new client, the professional accountant should not use or disclose confidential information obtained from a professional or business relationship.

However, confidential information may be disclosed in certain circumstances (figure 1), taking into account the following factors:

- degree of damage or prejudice to the interests of all parties, including third parties;
- relevance of the information and its substantiation, to the possible extent;
- intended mode of communication and the interlocutor.

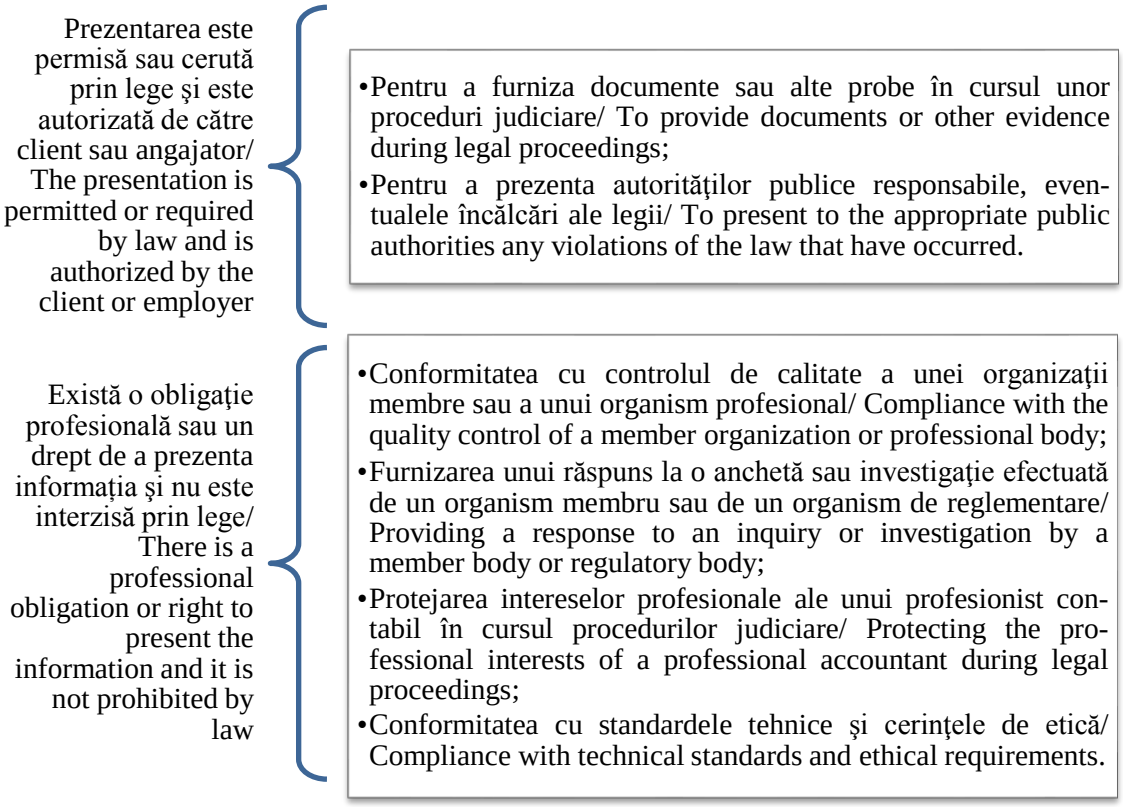


Figura 1. Circumstanțe adecvate de prezentare a informației confidențiale/
Figure 1. Appropriate circumstances for the disclosure of confidential information
Sursa: *elaborată de autor în baza [11, pp. 22-23]/*
Source: *developed by the author based on [11, pp. 22-23]*

Subliniem faptul că profesioniștii contabili trebuie să respecte confidențialitatea informațiilor chiar și într-un mediu social, deoarece riscul producerii unor scurgeri de informații poate apărea în diverse situații. Odată cu extinderea procesului de digitalizare, riscul scurgerii de informații confidențiale crește. Este important pentru fiecare profesionist contabil să cunoască mecanismele care pot duce la o informare frauduloasă. Actualmente, printre cele mai răspândite instrumente de extragere a informației confidențiale sunt:

1) frauda „Boss Scam" (mesaj de la șef) – este țintită, de obicei, spre angajații responsabili de efectuarea plăților, care, fiind induși în eroare, sunt îndemnați să efectueze anumite transferuri. Astfel, un autor trimite un mesaj, pretinzând că este managerul angajatului și solicită efectuarea urgentă a unei plăți. Deseori angajatului i se cere nerespectarea procedurilor obișnuite de autorizare a plăților [6];

We emphasize that a professional accountant must respect confidentiality of information even in a social environment, as the risk of information leakage can arise in various situation. With the expansion of the digitization process, the risk of leakage of confidential information increases. It is important for every accounting professional to know the mechanisms that can lead to fraudulent information. Currently, among the most widespread tools for extracting confidential information, we can highlight:

1) "Boss Scam" fraud (message from the boss) – usually targets employees authorized to make payments, who, through misrepresentation, are induced to make a transfer. Thus, an author sends a message, claiming to be the employee's manager, and requests an urgent payment. The employee is often required to disregard normal payment authorization procedures [6];
2) invoice fraud – the employee is contracted by someone who claims to be a represen-

2) fraude cu facturi – angajatul este contractat de cineva care pretinde că este reprezentantul unui furnizor și solicită modificarea datelor bancare (numărul de cont, banca la care e deschis contul etc.) pentru plățile viitoare. Noul cont este deținut de pretinsul reprezentant al furnizorului [8, p. 16];
3) e-mail-uri tip „phishing" – se referă la mesaje false care induc în eroare destinatarii, în scopul divulgării de către aceștia a informației confidențiale (date personale, financiare, de securitate etc.). Aceste e-mail-uri pot arăta identic cu cele pe care le emite o bancă: imită logoul și designul mesajelor reale, utilizează un limbaj care sugerează urgența, solicită descărcarea unui atașament sau deschiderea unui link [1] .

Potrivit Raportului Agenției Uniunii Europene pentru Securitatea Rețelelor și Informațiilor (ENISA), scurgerile de informații reprezintă unul din riscurile cibernetice în creștere, în era digitalizării, acoperind o gamă variată de informații (date cu caracter personal, date de afaceri, secrete comerciale etc.). Scurgerile de informații sunt cauzate, de obicei, de acțiunile individuale ale unor persoane sau ca urmare a unei erori în procesele interne ale entității în cauză. Involuntar, o eroare tehnică sau o configurare greșită, de asemenea, poate provoca o scurgere de informații. Conform raportului ENISA, anume atacurile intenționate stau la baza celor mai multe scurgeri de informații (figura 2).

tative of a supplier and requests the modification of bank details (account number, bank where the account is opened, etc.) for future payments. The new account is owned by the purported representative of the supplier [8, p. 16];
3) "phishing" type e-mails – refer to false messages that mislead the recipients, with the aim of disclosing confidential information (personal, financial, security data, etc.). These emails may look identical to those issued by a bank, they mimic the logo and design of real messages, they use language that suggests urgency, they request to download an attachment or open a link [1].

According to the Report of the European Union Agency for Network and Information Security (ENISA), information leakages represent one of the growing cyber risks in the digital age, covering a wide range of information (personal data, business data, trade secrets, etc.). Information leakages are usually caused by the individual actions of individuals or as a result of an error in the internal processes of the entity concerned. Inadvertently, a technical error or misconfiguration can also be the cause an information leak. According to the ENISA report, intentional attacks are the basis of most information leaks (figure 2).

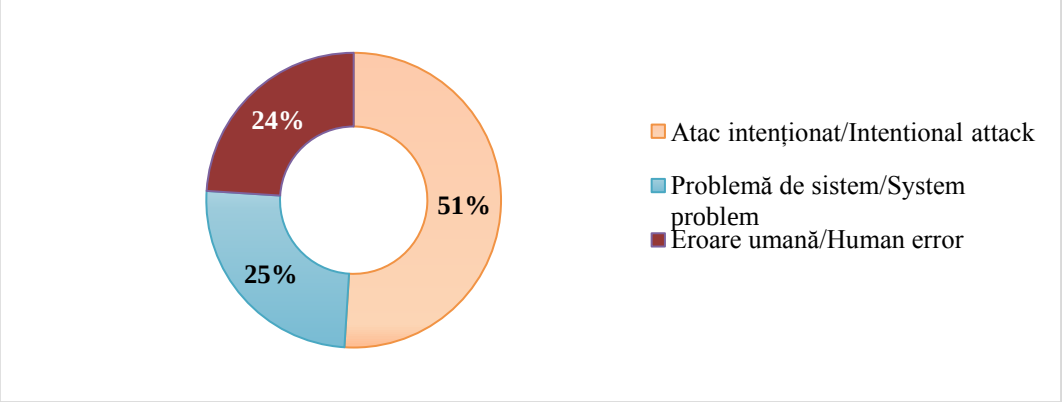


Figura 2. Cauzele principale ale divulgării informațiilor confidențiale la nivel internațional/ Figure 2. The main causes of confidential information disclosure at the international level
Sursa: *elaborată de autor în baza [13]/* ***Source:*** *developed by the author based on [13]*

În anul 2022 a avut loc o creștere semnificativă a scurgerilor de informații confidențiale (de 3,5 ori comparativ cu anul 2017), care poate fi explicată atât prin extinderea digitalizării, cât și de situația politică la nivel mondial (figura 3).

In 2022 there was a substantial increase in confidential information leakages (3.5 times compared to 2017), which can be explained both by the expansion of digitization and the political situation worldwide (figure 3).

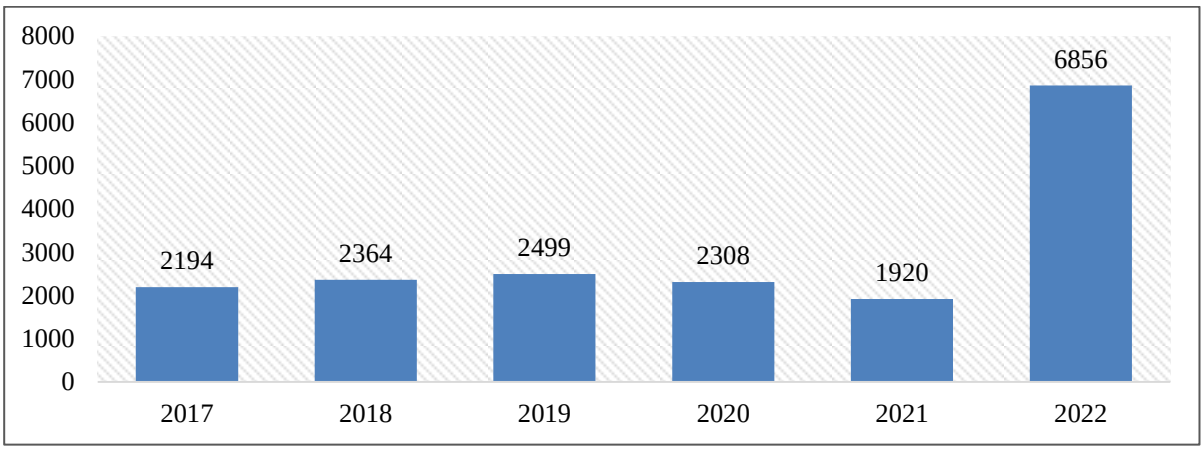


Figura 3. Numărul scurgerilor de informații confidențiale la nivel internațional, mlrd./
Figure 3. The number of confidential information leakage at the international level, billion
Sursa: *elaborată de autor în baza [12]/*
Source: *developed by the author based on [12]*

Din numărul total de scurgeri de informații, ponderea cea mai mare o dețin datele personale, fiind urmate de scurgeri informaționale aferente secretelor comerciale și celor de stat, iar, la final, se găsesc informațiile aferente diverselor plăți (figura 4).

Of the total number of information leakages, the largest share is held by personal data, followed by the leakages of information related to commercial and state secrets, then by various payments (figure 4).

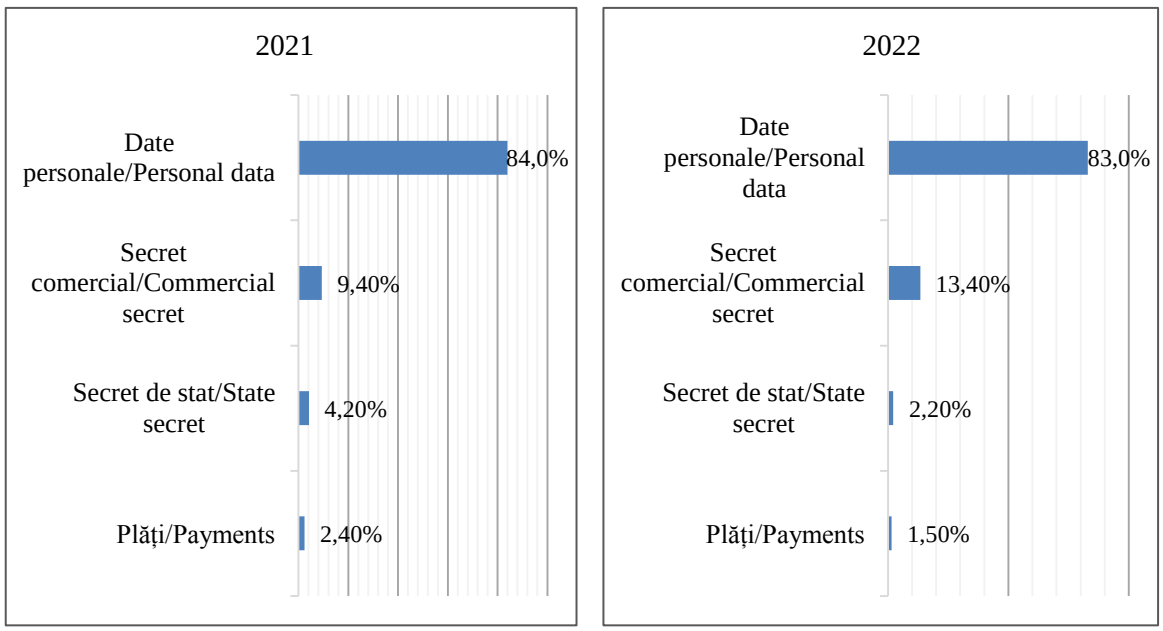


Figura 4. Distribuția scurgerilor de informații pe tipuri de date la nivel internațional /
Figure 4. Distribution of information leakages by data types at the international level
Sursa: *elaborată de autor în baza [12]/* ***Source:*** *developed by the author based on [12]*

Vectorul principal de atac în scurgerea de informații este reprezentat de intervențiile externe, care au manifestat o creștere constantă până în anul 2021, după care au scăzut brusc aproximativ cu 30%. Concomitent, are loc o scădere semnificativă a scurgerilor de informații din interior, ceea ce poate fi explicat prin măsurile luate cu privire la protecția datelor și restricționarea accesului către informațiile confidențiale. La fel, există un șir de scurgeri de informații din surse neidentificate, care a manifestat o creștere remarcabilă în anul 2022 (figura 5).

The main attack vector in information leakage is represented by external interventions, which showed a constant increase until the year 2021, after which they suddenly decreased by about 30%. At the same time, there is a significant decrease in the leakage of information from the inside, which can be explained by the measures taken regarding data protection and the restriction of access to confidential information. Likewise, there is a string of information leakages from unidentified sources that show a remarkable increase in the year 2022 (figure 5).

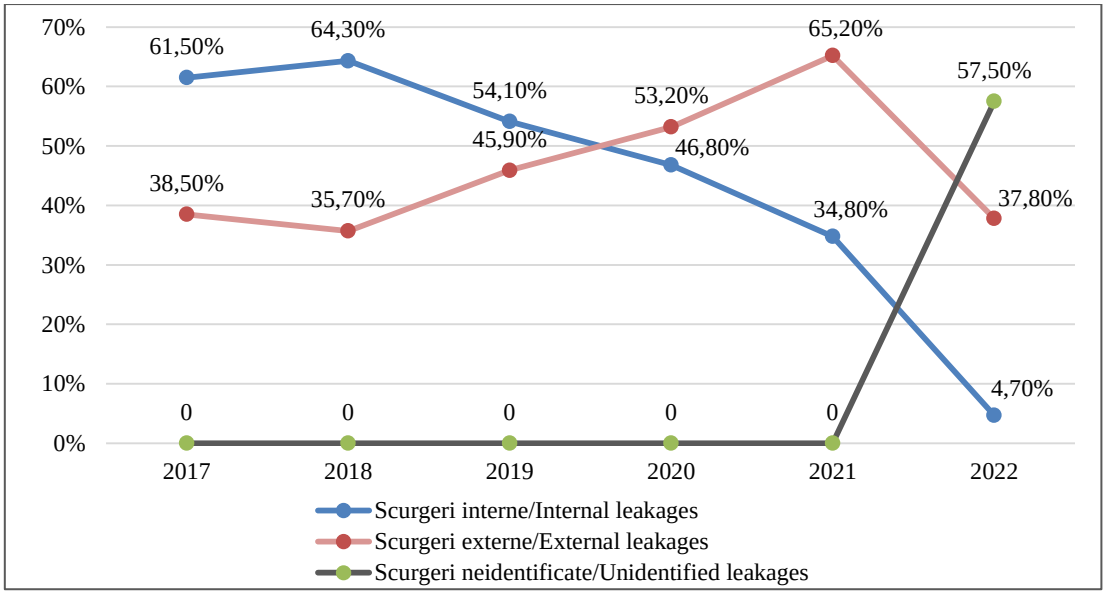


Figura 5. Vectorii scurgerilor de informații confidențiale la nivel internațional/
Figure 5. Vectors of confidential information leakages at the international level
Sursa: *elaborată de autor în baza [12]/*
Source: *developed by the author based on [12]*

Divulgarea informațiilor confidențiale reprezintă o amenințare pentru activitatea economică a unei societăți. Păstrarea datelor și informațiilor financiar-contabile constituie o obligație morală și juridică pentru persoanele care activează în cadrul acesteia. Divulgarea datelor și informațiilor confidențiale poate fi efectuată prin diverse metode: printr-o acțiune vădit intenționată sau printr-o inacțiune; în scris, oral, prin executarea și remiterea de copii, fotografii, imagini, prin scanare etc.; direct sau indirect (figura 6).

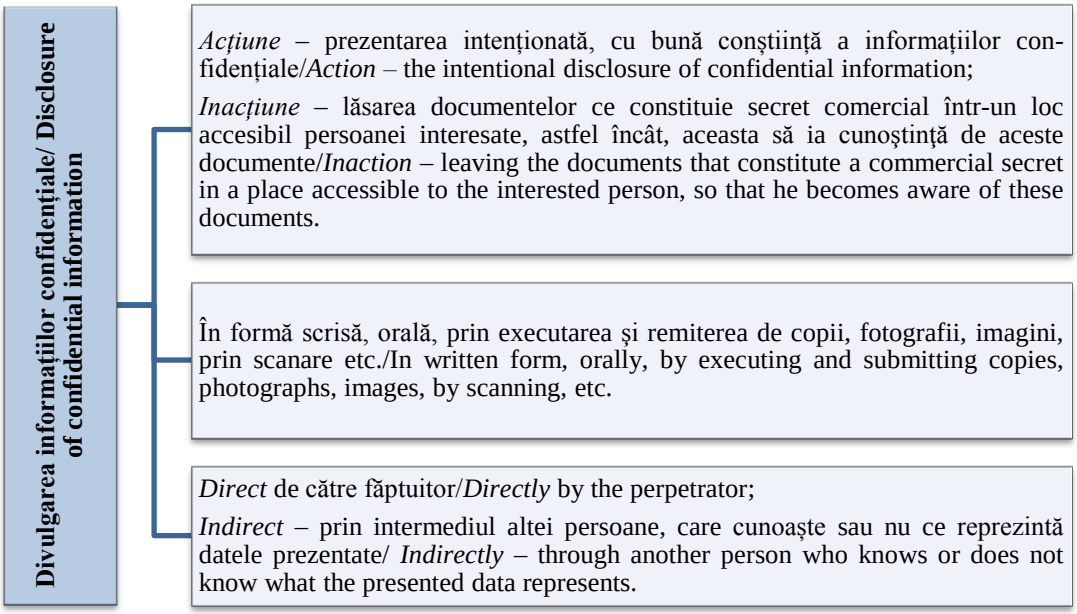
Divulgarea datelor și informațiilor confidențiale este urmată de sancționare, în conformitate cu prevederile legislației în vigoare. În cazul în care dezvăluirea unor astfel de date sau informații se face de către persoanele care le

The disclosure of confidential information represents a threat to the economic activity of the entity. The preservation of financial and accounting data and information is a moral and legal obligation for the people who work within it. The disclosure of confidential data and information can be carried out by various methods: by an obviously intentional action or by an inaction; in writing, orally, by executing and sending copies, photographs, images, by scanning, etc.; directly or indirectly (figure 6).

The disclosure of confidential data and information is followed by sanctions in accordance with the provisions of the legislation in force. In the situation where the disclosure of such data or information is due to the fault of a

cunoșteau prin natura atribuțiilor lor de serviciu, se constată, după caz, o infracțiune de neglijență, un abuz în serviciu sau o abatere disciplinară [9].

person who knew them by the nature of his duties, a crime of negligence or abuse in service or a disciplinary offence is established, as the case may be [9].



-

Figura 6. Modalități de divulgare a informațiilor confidențiale/
Figure 6. Ways of confidential information disclosure
Sursa: *elaborată de autor în baza [9]/*
Source: *developed by the author based on [9]*

Problema răspunderii disciplinare și materiale a angajatului pentru divulgarea datelor și informațiilor confidențiale și pentru alte fapte, ce au condus la scurgerea unor astfel de informații este reglementată de art. 327 și 328 din Codul muncii al Republicii Moldova [3].

Răspunderea administrativă este reglementată de art. 107 din Codul contravențional al Republicii Moldova „Obținerea sau divulgarea informațiilor care constituie secret comercial, bancar sau fiscal", care prevede sancționarea obținerii sau divulgării unor astfel de informații de către persoana căreia i-au fost încredințate aceste informații sau care le-a cunoscut prin atribuțiile de serviciu [2].

Răspunderea penală pentru divulgarea informațiilor confidențiale este prevăzută de art. 245^{10} din Codul penal al Republicii Moldova: „Obținerea ilegală sau divulgarea informațiilor ce constituie secret comercial sau bancar", care prevede atât pedeapsa cu amendă, cât și privarea de libertate [4].

The issue of disciplinary and material liability of the employee for the disclosure of confidential data and information and for other facts that led to the leakage of such information is regulated by art. 327 and 328 of the Labour Code of the Republic of Moldova [3].

Administrative liability is regulated by art. 107 of the Criminal Code of the Republic of Moldova, "Obtaining or divulging information that constitutes a commercial, banking or fiscal secret" which provides for the sanctioning of obtaining or divulging such information by a person to whom it was entrusted or became known to him through his duties [2].

Criminal liability for the disclosure of confidential information is provided by art. 245^{10} of the Criminal Code of the Republic of Moldova, "Illegal obtaining or disclosure of information that constitutes a commercial or banking secret" which provides for both a fine and deprivation of liberty [4].

În scopul protecției efective a informațiilor sale confidențiale, societatea trebuie: să elaboreze regulamente interne detaliate privind disciplina informațională; să prevadă în contractele de muncă clauze speciale privind protecția datelor și informațiilor confidențiale ale entității; să informeze angajații despre importanța protecției acestor informații și despre răspunderea juridică în cazul dezvăluirii lor.

Concluzii

În contextul celor relevate, menționăm că există date și informații cu caracter economic, care, deși nu constituie secrete de stat, nu sunt destinate publicului. Aceste date și informații trebuie păstrate cu strictețe, deoarece ele vizează interesele majore ale entităților și ale economiei naționale.

Este obligatorie conștientizarea necesității investițiilor în securitate, care au ca efect reducerea breșelor de securitate și, implicit, a atacurilor cibernetice și scurgerilor de informații. În scopul asigurării confidențialității, propunem elaborarea politicilor interne de securitate a datelor confidențiale, organizarea auditului sistemelor de securitate în cadrul entității, introducerea măsurilor de securitate a rețelelor și controlul accesului.

De obicei, misiunea asigurării securității informațiilor revine contabilului șef și administratorului entității. Contabilul șef, ca responsabil al sectorului financiar-contabil și, implicit, al sistemului de prelucrare automată a datelor, trebuie să asigure siguranța datelor entității, să fie conștient de faptul că nu trebuie să divulge informația pe care o deține unor persoane terțe, inclusiv rudelor și prietenilor, chiar și după încheierea afacerilor.

Un rol important în asigurarea confidențialității datelor revine organizării procesului de securitate, care are ca obiectiv asigurarea unei administrări unitare a informației în cadrul întreprinderii. Astfel, recomandăm managerilor entităților să se asigure că utilizatorii sistemului informațional, care au acces la date personale și confidențiale, respectă procedurile și politicile de securitate. Totodată, organizarea securității informaționale nu trebuie să se limiteze doar la personalul intern, dar și la persoanele terțe, fiind recomandată implementarea unui proces care să controleze accesul terților.

In order to effectively protect their confidential information, entities should develop detailed internal regulations on information discipline, provide in employment contracts special clauses on the protection of data and confidential information of the entity, inform employees about the importance of protecting this information and about legal liability in the case of its disclosure.

Conclusions

Considering everything that has been revealed, we can mention that there are data and information of an economic nature which, although they do not constitute state secrets, are nevertheless not intended for the public. These data and information must be kept strictly because they target important interests of both the entities and the national economy.

It is strictly necessary to be aware of the need for investments in security at the entity level, which has the effect of reducing security breaches and implicitly cyber-attacks and information leakages. Among the most accessible measures to ensure confidentiality, we can highlight the development of confidential data security policies, the audit of security systems, the introduction of security measures in networks and access control.

Typically, the task of ensuring information security is attributed to the chief accountant and the administrator of the entity. The chief accountant, as the person in charge of the financial and accounting sector and implicitly of the automatic data processing system, has the obligation to ensure the confidentiality of the entity's data, so he must be aware of the fact that he must not disclose the information he holds to third parties, including relatives and friends, even after the end of the business relationship.

An important role in ensuring data confidentiality belongs to the organization of the security process whose objective is to ensure a unified administration of information within the enterprise. Thus, we recommend that entity managers ensure that users of the information system who have access to personal and confidential data comply with security procedures and policies. At the same time, the organization of information security must not be limited only to internal staff, but also to third parties, and it is recommended to implement a process by which third party access is controlled.

Bibliografie/ Bibliography:

1. *Avoid and report phishing emails* [online]. [citat 26.04.2023]. Disponibil: https://support.google.com/mail/answer/8253?hl=en
2. Codul Contravențional al Republicii Moldova: nr. 218 din 24.10.2008. *Registrul de stat al actelor juridice* [bază de date online]. [citat 02.04.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=125094&lang=ro
3. Codul Muncii al Republicii Moldova: nr. 154 din 28.03.2003. *Registrul de stat al actelor juridice* [bază de date online]. [citat 15.04.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=113032&lang=ro
4. Codul Penal al Republicii Moldova nr. 985 din 18.04.2002. *Registrul de stat al actelor juridice* [bază de date online]. [citat 16.05.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=109495&lang=ro
5. DOLGHIN, N.; SARCINSCHI, A.; DINU, M. S. *Riscuri și amenințări la adresa securității României. Actualitate și perspectivă*. București: Editura Universitatea Națională de Apărare, 2004. 24 p. ISBN 973-663-143-5.
6. FAKHAR, I. Phishing technique: Message from the boss. *INFOSEC* [online]. [citat 18.04.2023]. Disponibil: https://resources.infosecinstitute.com/topic/phishing-technique-message-from-the-boss/
7. FORNEA, D. Identitatea digitală, suveranitatea datelor și calea către o tranziție digitală echitabilă pentru cetățenii care trăiesc în societatea informațională. *Comitetul Economic și Social European* [online]. [citat 06.04.2023]. Disponibil: https://www.eesc.europa.eu/ro/our-work/opinions-information-reports/opinions/digital-identity-data-sovereignty-and-path-towards-just-digital-transition-citizens-living-information-society
8. FAIR ISAAC CORPORATION (FICO). *Fraud in the World of Real-Time Payments*. [online]. 2018. [citat 21.04.2023]. Disponibil: https://www.fico.com/sites/default/files/2018-06/FICO_Fraud_in_the_World_of_Real-Time_Payments_4543WP_EN.pdf
9. IUSTIN, Viorel. *Secretul comercial. Invitație la tăcere*. [online]. [citat 17.05.2023]. Disponibil: https://www.bizlaw.md/2017/08/04/secretul-comercial-invitatie-la-tacere
10. LUCHICI, A. Digitalizarea – o necesitate pentru a rămâne competitivi pe termen lung. *Linkedin* [online]. 2020. [citat 12.04.2023]. Disponibil: https://ro.linkedin.com/pulse/digitalizarea-o-necesitate-pentru-r%C4%83m%C3%A2ne-competitivi-pe-luchici
11. *Manualul Codului Etic Internațional pentru Profesioniștii Contabili*. Bucureşti: IFAC, 2021. [online]. [citat 22.04.2023]. Disponibil: https://www.ifac.org/_flysystem/azure-private/publications/files/2021-IESBA-Handbook_RO_Secure.pdf
12. *Raport de investigare privind scurgerile de informații confidențiale.* Centrul analitic InfoWatch Expert, 2022. [online] [citat 28.04.2023]. Disponibil: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf
13. *Raportul ENISA privind situația amenințărilor scurgerilor de informații*. 2020. [online]. [citat 23.04.2023]. Disponibil: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
14. RÎNDAŞU, Sînziana-Maria. Securitatea informațiilor contabile – o analiză a percepției practicienilor din România. *Audit Financiar*. 2019, vol. 17, nr. 2(154), pp. 298-305. ISSN 1583-5812, ISSN on-line: 1844-8801.