DIGITALIZAREA ÎN DOMENIUL SĂNĂTĂȚII ȘI PROTECȚIA DREPTURILOR PACIENȚILOR: ANALIZA RISCURILOR ȘI MĂSURILE DE CONTRACARARE

DIGITALIZATION OF HEALTHCARE AND PATIENT RIGHTS PROTECTION: RISK ANALYSIS AND COUNTERMEASURES

CZU: 34:614.253.83:004.77 **DOI:**https://doi.org/10.59295/ssdoed2024.21

Constantin PISARENCO[1]

ABSTRACT. *Research Objective: Comprehensive analysis of the impact of digitalization on patients' rights and safety in the context of legal violations in healthcare.*

Materials and Methods: Analysis of relevant domestic and foreign literature sources, as well as normative legal acts, was conducted. Literature search was carried out in scientific libraries and the informational legal system "State Register of Legal Acts of the Republic of Moldova."

Results and Discussion: Identified two key aspects of the impact of digital technologies on healthcare: positive changes, such as improved accessibility and personalization of medical services, and negative consequences, including the growth of cyber threats and data confidentiality issues. Discussed the need for a comprehensive approach to mitigate these risks, combining technological, organizational, and legal measures. The importance of future research on the impact of the latest technologies on data security and patients' rights is noted.

Conclusion: Digital technologies have improved healthcare but created challenges, including cyber threats, which require an integrated approach that combines technology, law, and education, as well as public-private partnerships and international community.

Keywords: *healthcare, digitalization, patient rights, medical law*

REZUMAT. *Scopul cercetării. Analiza cuprinzătoare a impactului digitalizării asupra drepturilor și securității pacienților în contextul infracțiunilor din domeniul sănătății.*

Materiale și metode. S-a efectuat o analiză a surselor relevante din literatura națională și internațională, precum și a actelor normative. Cercetarea literaturii de specialitate a fost efectuată în biblioteci și în sistemul informațional juridic de referință "Registrul de stat al actelor juridice al Republicii Moldova".

Rezultate și discuție. Au fost identificate două aspecte cheie ale impactului tehnologiilor digitale asupra domeniului sănătății: schimbări pozitive, cum ar fi îmbunătățirea accesului și individualizarea serviciilor medicale, și a consecințelor negative, inclusiv creșterea amenințărilor cibernetice și probleme legate de confidențialitatea datelor. S-a discutat necesitatea unei abordări complexe pentru atenuarea acestor riscuri, care să combine măsuri tehnologice, organizatorice și legale. S-a subliniat importanța cercetărilor viitoare referitoare la impactul celor mai noi tehnologii asupra securității datelor și drepturilor pacienților.

Concluzie. Tehnologiile digitale au îmbunătățit sistemul de sănătate, dar au creat provocări, inclusiv amenințări la adresa securității cibernetice, care necesită o abordare integrată,

[1] Constantin PISARENCO, Universitatea Liberă Internațională din Moldova, ORCID ID: 0000-0001-5548-4653, e-mail: constantin.pisarenco@gmail.com

care să includă tehnologia, legea și educația, precum și parteneriatele public-privat și comunitatea internațională.

Cuvinte-cheie: *sănătate, digitalizare, drepturile pacienților, drept medical.*

Introducere

În contextul evoluției globale către digitalizare, asistența medicală nu face excepție. Digitalizarea în acest domeniu reprezintă un progres semnificativ în ceea ce privește acordarea de asistență medicală calitativă. Acest proces implică adoptarea diferitelor tehnologii, cum ar fi fișele medicale electronice, telemedicina, aplicațiile mobile de sănătate și utilizarea inteligenței artificiale pentru diagnosticare și tratament. Aceste inovații contribuie la îmbunătățirea accesului la serviciile de sănătate, la creșterea eficienței tratamentului și la optimizarea activității personalului medical.

Telemedicina, de exemplu, permite asistența medicală la distanță, ceea ce este deosebit de important în regiunile îndepărtate și cele cu venituri mici. Fișele medicale electronice facilitează stocarea, accesul și gestionarea informațiilor medicale și contribuie la îmbunătățirea calității asistenței medicale prin diagnosticarea mai precisă și mai rapidă.

Pe lângă beneficii, însă, digitalizarea aduce și anumite riscuri. Aspectele privind confidențialitatea și securitatea datelor devin din ce în ce mai importante, deoarece scurgerile de informații și accesul neautorizat la informațiile medicale pot avea consecințe nevaforabile pentru pacienți și furnizorii de servicii medicale. În acest context, elaborarea și punerea în aplicare a unor măsuri de securitate și standarde de confidențialitate fiabile devine o provocare cheie pentru asistența medicală în era digitală.

Perspectivele digitalizării în domeniul sănătății sunt vaste și includ nu numai îmbunătățirea practicilor actuale de gestionare a sănătății, ci și dezvoltarea de noi abordări și tehnologii. Inteligența artificială și machine learning pot schimba radical metodele de diagnosticare și tratament, oferind soluții personalizate pentru fiecare pacient. Este important ca aceste inovații să meargă mână în mână cu asigurarea securității și confidențialității datelor pacienților.

Literatura de specialitate a abordat în ultima vreme în mod special aspecte cheie ale problemei, precum importanța unor măsuri sporite de securitate cibernetică, crearea de standarde pentru protejarea vieții private și rolul principiilor etice în gestionarea datelor pacienților. Subiectul devine deosebit de important în contextul unor incidente recente de mare amploare care au implicat încălcări ale securității datelor și utilizarea ilegală a informațiilor medicale.

Obiectivul cercetării. O analiză cuprinzătoare a impactului digitalizării asupra drepturilor și siguranței pacienților în contextul infracțiunilor din domeniul sănătății.

Studiul își propune să contribuie la o mai bună înțelegere a relației dintre procesul de dezvoltare a digitalizării în domeniul asistenței medicale și necesitatea de a

asigura siguranța pacienților, oferind modalități de abordare a provocărilor actuale și viitoare în acest domeniu.

Materiale și metode

Au fost analizate surse relevante din literatura de specialitate națională și internațională, precum și actelor juridice. Căutarea literaturii a fost efectuată în bibliotecile științifice eLIBRARY, PubMed, Scopus Database prin interogări cheie. Căutarea actelor juridice în vigoare în Republica Moldova a fost efectuată în sistemul informațional juridic de referință "Registrul de stat al actelor juridice din Republica Moldova".

Rezultate și discuție

Tendințele moderne de dezvoltare a societății contemporane de civilizație mondială în ultimul deceniu au făcut un salt calitativ de la modelul post-industrial la o nouă eră a economiei digitale, caracterizată prin integrarea tehnologiilor avansate de informare și comunicare [1].

Procesul de diseminare a noilor tehnologii și de digitalizare a diferitelor sfere ale economiei și vieții sociale afectează în mod direct îmbunătățirea practicilor medicale. Cercetătorii remarcă faptul că toate elementele sistemului de sănătate se confruntă astăzi cu o revoluție digitală [2].

Din punct de vedere al istoriei și al prezentului, tehnologiile digitale în domeniul sănătății se caracterizează prin faptul că tehnologiile digitale au început să pătrundă în medicină încă din a doua jumătate a secolului al XX-lea, dar dezvoltarea semnificativă și utilizarea lor pe scară largă au avut loc în ultimele decenii.

Parcursul istoric al digitalizării în domeniul sănătății poate fi urmărit de la primele sisteme computerizate de gestionare a datelor medicale până la soluțiile digitale integrate moderne, cum ar fi fișele medicale electronice, sistemele de asistență pentru decizii clinice și telemedicina.

Anii 1970 și 1980 s-au caracterizat prin introducerea tehnologiei computerizate pentru gestionarea informațiilor medicale, care a pus bazele dezvoltării ulterioare a fișelor medicale electronice. În anii 1990, odată cu dezvoltarea internetului și creșterea capacității de procesare, tehnologiile digitale au devenit mai accesibile și mai funcționale, ceea ce a dus la o aplicare mai largă a acestora în domeniul sănătății.

La începutul secolului XXI, odată cu dezvoltarea continuă a tehnologiei IT, a început o nouă etapă de digitalizare în domeniul sănătății, inclusiv introducerea telemedicinei, a aplicațiilor mobile în domeniul sănătății și a utilizării inteligenței artificiale. Aceste inovații au extins în mod semnificativ posibilitățile de îngrijire medicală, asigurând o mai mare accesibilitate, precizie și eficiență a tratamentului [3].

Creșterea influenței a două tehnologii - big data (BD) și inteligența artificială (AI) - este deosebit de importantă. Big data acumulează informații utile despre un număr mare de entități unice, modele structurale, deficiențe și procesul de luare a

deciziilor într-o gamă largă de aplicații digitale diverse; inteligența artificială face prognoze, elaborează recomandări și realizează modelarea proceselor.

Combinația dintre big data și inteligența artificială, de exemplu sub forma aplicațiilor de machine learning, deschide noi orizonturi pentru medicina individualizată și analiza predictivă, schimbând radical abordările privind diagnosticarea, tratamentul și prevenirea bolilor. Cu toate acestea, tehnologia integrată BD&AI implică, de asemenea, riscuri pentru utilizatori legate de încălcarea confidențialității și nu numai.

În contextul evoluției rapide a sistemului de sănătate de azi, digitalizarea fișelor medicale a devenit o piatră de temelie a sistemelor moderne de asistență medicală. Înregistrările medicale electronice (EMR) [4] și fișele medicale electronice (EHR) permit stocarea și gestionarea centralizată a informațiilor medicale ale pacienților, îmbunătățind calitatea îngrijirii și reducând probabilitatea de erori [5].

Telemedicina este o componentă importantă a procesului global de digitalizare în domeniul sănătății. Apariția sa se datorează în mare măsură dezvoltării tehnologiilor moderne de telecomunicații. Telemedicina oferă consultanță și tratament medical la distanță, ceea ce este deosebit de important în zonele cu acces limitat la serviciile de sănătate, jucând, de asemenea, un rol important în pandemia COVID-19 [6-8].

Asistența medicală mobilă este un sector nou, orientat mai degrabă către persoanele implicate activ în îngrijirea sănătății în scop preventiv decât către pacienți. Cu ajutorul unor aplicații speciale, o persoană își poate monitoriza în mod independent sănătatea și indicatorii fiziologici. Acest lucru permite ca persoana să fie informată și independentă față de medic, permițându-i să ia decizii independente cu privire la sănătatea sa, la prevenirea bolilor.

Aceste tehnologii și inovații continuă să evolueze, având un impact semnificativ asupra tuturor aspectelor asistenței medicale și oferind instrumente puternice pentru a îmbunătăți calitatea îngrijirii și accesul la serviciile de sănătate. Cu toate acestea, pe măsură ce crește dependența față de tehnologia digitală, crește și necesitatea unor măsuri stricte de protecție a datelor și a confidențialității pacienților.

Drepturile pacienților în era medicinei digitale reprezintă un ansamblu de norme fundamentale menite să protejeze drepturile și să asigure bunăstarea persoanelor în timp ce primesc îngrijiri medicale, reglementate la nivel internațional prin norme de convenții, directive, rezoluții, recomandări, principii [9, 10].

Aceste drepturi acoperă o gamă largă de garanții, de la accesul la asistență medicală de calitate, care include dreptul fiecărui pacient de a consulta medici specialiști profesioniști și de a primi un tratament adecvat, până la respectarea demnității personale și a confidențialității [11-15].

Pacienții au dreptul de a fi pe deplin informați cu privire la starea lor de sănătate, inclusiv diagnosticul, tratamentele propuse și posibilele riscuri, precum și dreptul de a avea acces la informațiile privind sănătatea lor. Deosebit de importantă în era digitalizării este protecția informațiilor medicale personale ale pacienților, asigurând confidențialitatea și protecția acestora împotriva accesului neautorizat.

Printre drepturile esențiale ale pacienților se numără și dreptul la acordul informat, care presupune că pacientul este pe deplin conștient de toate aspectele tratamentului care urmează să fie furnizat, inclusiv obiectivele, riscurile și alternativele posibile. Dreptul de a fi respectat, care include luarea în considerare a convingerilor culturale, religioase și a preferințelor personale ale pacienților, este, de asemenea, un aspect important al relației dintre profesioniștii din domeniul sănătății și pacienți.

În era digitală, se acordă o atenție deosebită informării pacienților cu privire la drepturile și obligațiile care le revin atunci când apelează la serviciile medicale digitale. Pacienții trebuie să fie informați cu privire la modul în care sunt utilizate datele lor, la măsurile de protecție existente și la măsurile pe care le pot lua pentru a-și proteja viața privată. Aceasta pentru a se asigura că beneficiile digitalizării sunt realizate fără a compromite viața privată și drepturile pacienților. Recunoașterea și respectarea acestor drepturi este parte integrantă a unor relații demne și etice între profesioniștii din domeniul sănătății și pacienți și contribuie la menținerea unor standarde înalte de îngrijire a pacienților.

Impactul digitalizării în domeniul sănătății asupra vieții private și a accesului la informațiile medicale are două aspecte. În primul rând, tehnologiile digitale, inclusiv fișele medicale electronice și platformele de telemedicină, oferă un acces mai bun la informațiile privind sănătatea atât pentru profesioniștii din domeniul sănătății, cât și pentru pacienți, simplificând procesul de diagnosticare și tratament și permițând pacienților să fie mai bine informați cu privire la sănătatea lor. Acest lucru încurajează o mai mare participare a pacienților la luarea deciziilor privind propriul tratament. În schimb, digitalizarea sporește riscurile asociate cu confidențialitatea datelor.

Scurgerile de date, atacurile cibernetice și accesul neautorizat la informațiile personale privind starea de sănătate pot avea consecințe nefavorabile asupra confidențialității pacienților, în special în contextul stocării în cloud și al transferului de date între sisteme [16]. Pentru a proteja confidențialitatea pacienților în era digitală, multe țări au elaborat cadrul legislativ și de reglementare strict care stabilește cerințe pentru prelucrarea și protecția datelor cu caracter personal, inclusiv a informațiilor medicale, și subliniază importanța acordului informat al pacienților atunci când datele lor sunt utilizate.

Riscurile și amenințările la adresa securității în domeniul sănătății digitale presupun două aspecte, întrucât procesul de digitalizare aduce îmbunătățiri semnificative în privința gestionării asistenței medicale, dar sporește și riscurile și amenințările la adresa securității datelor, printre care se numără atacurile cibernetice, spargerile de date și accesul neautorizat.

În prezent, experții evaluează nivelul de securitate a datelor cu caracter personal în instituțiile de sănătate publice și private ... ca fiind scăzut. Acest fapt se datorează calificării insuficiente a personalului, lipsei unui sistem unificat de protecție a informațiilor și nivelului insuficient de control. Soluționarea acestor probleme necesită o reglementare clară a statului și introducerea de noi software [17].

Instituțiile medicale și sistemul de sănătate sunt ținte tentante pentru infractorii cibernetici din cauza cantității mari de informații sensibile pe care le procesează. Atacurile cibernetice pot lua mai multe forme, inclusiv viruși, troieni, phishing și atacuri malware, inclusiv ransomware. Aceste atacuri pot perturba sistemele medicale, pot cauza pierderi de date și chiar pot pune în pericol viața pacienților dacă afectează dispozitive medicale vitale.

Breșele de securitate pot apărea nu numai ca urmare a unor atacuri externe, ci și din cauza unor vulnerabilități interne, cum ar fi erori de software, deficiențe în protocoalele de protecție a datelor sau erori umane. Breșele de date pot implica nu numai divulgarea de informații medicale ale pacienților, ci și de date financiare ale acestora, ceea ce sporește riscul de fraudă și de încălcare a confidențialității.

Accesul neautorizat la datele medicale poate fi realizat atât de atacatori externi, cât și de angajați ai unităților sanitare. Acest lucru poate include vizualizarea fișelor medicale electronice fără a avea o autorizație, ceea ce încalcă confidențialitatea pacienților și subminează încrederea în instituțiile medicale. Este important să se asigure existența unor măsuri stricte de control al accesului și de monitorizare pentru a preveni astfel de incidente.

Pentru a minimiza în mod eficient riscurile de securitate și amenințările la adresa asistenței medicale în era digitală, este important să se adopte o abordare integrată a măsurilor de securitate. Aceasta include actualizări și audituri de securitate regulate, instruirea personalului, utilizarea unei criptări puternice și a unei autentificări cu factor multiplu, precum și elaborarea și punerea în aplicare a unor planuri de reacție la incidente de securitate. Conștientizarea și răspunsul adecvat la amenințări necesită nu numai soluții tehnologice, ci și măsuri juridice, organizaționale și educaționale.

Pentru a înțelege mai bine amenințările reale pe care le reprezintă digitalizarea în domeniul sănătății, este util să analizăm exemple specifice de incidente privind securitatea datelor.

În mai 2017, un atac cibernetic care a utilizat virusul WannaCry a afectat grav unitățile sanitare din întreaga lume, inclusiv Serviciul Național de Sănătate (NHS) din Regatul Unit. Atacul a criptat înregistrările medicale electronice, a perturbat echipamentele și a anulat mii de programări medicale. Acest incident a evidențiat importanța actualizărilor regulate ale software-ului și a backup-urilor de date [18].

În 2018, Singapore s-a confruntat cu una dintre cele mai mari breșe de date din domeniul sănătății, care a afectat peste 1,5 milioane de pacienți, inclusiv pe primministrul țării. Atacatorii au obținut acces la date cu caracter personal și la fișele electronice de sănătate. Acest caz a arătat cât de importante sunt măsurile de securitate complete, inclusiv monitorizarea și intervenția în caz de incidente [19].

În 2018, MyFitnessPal, o aplicație mobilă utilizată pentru a urmări activitatea fizică și dieta, a fost spartă, compromițând datele a 150 de milioane de utilizatori. Deși aplicația nu este în mod explicit medicală, ea conține date care pot fi utilizate pentru a crea un profil detaliat al sănătății unei persoane [20].

Aceste exemple arată că amenințările la adresa securității informațiilor pot avea consecințe semnificative, inclusiv încălcări ale confidențialității, daune materiale și chiar riscuri care pun în pericol viața. Ele subliniază necesitatea unei abordări cuprinzătoare a securității cibernetice, care să includă strategii tehnologice, administrative și educaționale.

Unul dintre principalele tipuri de infracțiuni în domeniul sănătății în era digitală este reprezentat de atacurile cibernetice asupra instituțiilor medicale și de încălcarea securității datelor. Atacatorii pot folosi datele sustrase într-o varietate de scopuri, inclusiv vânzări pe piața neagră, fraudă de identitate și escrocherie.

Frauda în domeniul asigurărilor de sănătate devine din ce în ce mai răspândită și mai sofisticată în era digitală. Infractorii folosesc fișele medicale electronice sustrase sau falsificate pentru a face cereri false către companiile de asigurări. Acest lucru nu numai că provoacă pierderi financiare, dar poate duce, de asemenea, la un tratament necorespunzător al pacienților din cauza unor fișe medicale denaturate.

Accesul și utilizarea neautorizată a informațiilor privind sănătatea devin, de asemenea, o problemă. Aceasta poate include accesul la informații sensibile despre pacienți fără consimțământ sau utilizarea acestor informații în scopuri ilegale, cum ar fi angajarea, discriminarea sau acordarea de credite.

Odată cu dezvoltarea dispozitivelor medicale conectate, riscul de compromitere a datelor crește. Piratarea unor astfel de echipamente poate perturba funcționarea acestora, punând în pericol sănătatea și viața pacienților.

În era digitală, distribuirea medicamentelor falsificate sau obținute ilegal prin intermediul farmaciilor online devine o problemă gravă. Aceasta include vânzarea de medicamente contrafăcute care pot fi ineficiente sau chiar periculoase pentru sănătate.

Încălcările în domeniul telemedicinei, inclusiv furnizarea de informații medicale false sau obținerea de servicii medicale cu rea-credință, devin, de asemenea, o provocare. Astfel de acțiuni pot include utilizarea datelor altor persoane pentru a obține consultanță medicală sau pentru a obține medicamente. Atacatorii pot nu numai să intervină și să divulge informații personale sensibile, ci și să dezvolte un soft care să interfereze, de exemplu, cu sistemele de susținere a vieții corpului uman. Consecințele ar fi atunci mai grave [21].

Aceste infracțiuni demonstrează că digitalizarea asistenței medicale necesită nu numai inovații tehnologice, ci și măsuri de securitate sporite și dezvoltarea cadrului juridic și etic pentru a proteja datele și a preveni comiterea de infracțiuni în domeniul sănătății.

Infracțiunile din domeniul sănătății în era digitală sunt caracterizate de o varietate de motive și metode. Aceste infracțiuni pot fi determinate de obținerea de câștiguri financiare, obținerea de informații personale sau sensibile, frauda în domeniul asigurărilor, vânzarea de informații medicale sustrase pe piața neagră sau extorcarea de bani prin amenințarea cu divulgarea de informații confidențiale.

Infractorii pot căuta să acceseze datele medicale pentru a obține informații despre persoane, care pot fi apoi folosite pentru obținerea unui credit. În acest caz, fișele medicale sunt o sursă importantă de informații personale.

Metodele de comitere a infracțiunilor în domeniul sănătății includ atacuri cibernetice precum phishing, piratarea parolelor, utilizarea de software malițios și atacuri asupra dispozitivelor medicale. Astfel de atacuri pot avea ca scop accesarea sistemelor medicale pentru a sustrage datele sau pentru a perturba funcționarea acestora.

În unele cazuri, infracțiunile din domeniul sănătății sunt comise de personalul medical care abuzează de accesul lor la sistemele informatice. Acest lucru poate include vizualizarea nejustificată a informațiilor confidențiale sau permiterea accesului unor terți la aceste informații.

Înțelegerea acestor motive și metode este esențială pentru dezvoltarea unor strategii eficiente de prevenire și combatere a infracțiunilor din domeniul sănătății în era digitală. Aceasta include atât măsuri de securitate tehnică, cât și consolidarea standardelor juridice și etice.

Digitalizarea în domeniul sănătății și amenințările de securitate aferente au un impact semnificativ atât asupra pacienților, cât și asupra furnizorilor de servicii medicale. Aceste efecte pot varia de la daune materiale până la daune morale.

Scurgerile de date și alte încălcări ale securității pot avea consecințe nefavorabile pentru pacienți, inclusiv compromiterea vieții private, pierderi financiare și chiar amenințări asupra sănătății fizice.

În plus, sustragerea de informații personale și financiare poate duce la fraudă și furt de identitate.

Pentru furnizorii de servicii medicale, atacurile cibernetice și scurgerile de date pot duce la pierderi financiare semnificative, la întreruperea activității și la neîncrederea pacienților. De exemplu, atacurile de tip ransomware pot paraliza sistemele medicale, ceea ce, la rândul lor, poate îngreuna furnizarea de asistență medicală în timp util. În plus, furnizorii de servicii medicale se pot confrunta cu acțiuni în instanță și cu prejudicii de reputație în cazul unor spargeri de date ale pacienților.

Recuperarea în urma atacurilor cibernetice sau a încălcărilor de date necesită resurse financiare și de timp semnificative. Instituțiile trebuie să investească în măsuri de securitate sporite, în audituri și în formarea personalului, precum și în gestionarea consecințelor încălcărilor, inclusiv în asistență juridică și asigurarea unei bune gestionări a reputației.

Evaluarea și gestionarea acestor riscuri este esențială pentru a asigura siguranța și securitatea serviciilor de asistență medicală în era digitală.

Protecția juridică a confidențialității și securității datelor medicale în era digitală

Legislația internațională și națională a fost elaborată ca răspuns la provocările privind confidențialitatea și securitatea datelor în era digitală. Aceste acte au ca scop

protejarea drepturilor pacienților și asigurarea utilizării sigure a informațiilor medicale.

General Data Protection Regulation (GDPR) al Uniunii Europene stabilește cerințe pentru prelucrarea datelor cu caracter personal ale cetățenilor UE, inclusiv a informațiilor privind starea de sănătate [22]. Acest regulament oferă dreptul de a accesa, de a rectifica, de a șterge și de a transfera datele și impune organizațiilor să obțină un consimțământ clar și specific pentru a prelucra datele.

Health Insurance Portability and Accountability Act (HIPAA) din SUA reglementează prelucrarea și difuzarea informațiilor medicale, asigurând confidențialitatea și securitatea datelor medicale personale [23]. Această lege impune standarde de protecție a datelor și solicită furnizorilor de servicii medicale și partenerilor acestora să ia măsurile necesare pentru a proteja informațiile de sănătate ale pacienților.

Multe țări și-au elaborat propriile legi privind protecția datelor, ținând cont de particularitățile sistemelor juridice naționale și ale contextelor culturale. De exemplu, în Regatul Unit se aplică *Data Protection Act 2018* [24], în Rusia este *Legea federală privind datele cu caracter personal* [25], iar în Republica Moldova este *Legea privind protecția datelor cu caracter personal* [26].

În plus față de legislația națională, există instrumente internaționale, cum ar fi *Declarația Universală a Drepturilor Omului a ONU* [27] și *Convenția Europeană a Drepturilor Omului* [28], care influențează, de asemenea, protecția datelor cu caracter personal și a drepturilor pacienților la nivel global.

În plus față de legislație, organizațiile internaționale, cum ar fi Organizația Mondială a Sănătății și Organizația Internațională pentru standardizare, elaborează standarde și ghiduri pentru a îmbunătăți securitatea și confidențialitatea datelor medicale. Aceste standarde și recomandări oferă îndrumare organizațiilor din domeniul sănătății și companiilor IT pentru dezvoltarea și implementarea unor soluții digitale sigure.

Analiza contextului juridic al digitalizării sistemului național de sănătate indică faptul că, în conformitate cu legislația Republicii Moldova, persoanele care încalcă cerințele *Legii privind protecția datelor cu caracter personal*, în funcție de circumstanțele individuale și de gravitatea infracțiunii comise.

Astfel, în *Codul penal al Republicii Moldova* [29], un capitol distinct este dedicat infracțiunilor în domeniul informației și telecomunicațiilor, articolele acestuia reglementează aspecte ce țin de securitatea și confidențialitatea datelor

Articolul 259. *Accesul ilegal la informația* computerizată prevede pedeapsa pentru accesul ilegal la informația computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de

dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice şi dacă a cauzat daune în proporţii mari,

Acest lucru este deosebit de important în contextul datelor medicale, deoarece accesul neautorizat la astfel de informații poate duce la breșe în ceea ce privește confidențialitatea și securitatea pacienților.

Articolele 260, 260.1-260.6 vizează o gamă largă de infracțiuni care țin de securitatea informațiilor, Interceptarea ilegală a unei transmisii de date informatice, Alterarea integrităţii datelor informatice ţinute într-un sistem informatic, perturbarea funcţionării sistemului informatic, Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor codurilor de acces sau a datelor similar.

În contextul sănătății digitale, aceste articole contribuie la protejarea datelor medicale împotriva utilizării abuzive și oferă protecție din punct de vedere juridic a informațiilor despre pacienți.

Articolul 261. *Încălcarea regulilor de securitate a sistemului informatics* și Articolul 261.1 Accesul neautorizat la reţelele şi serviciile de telecomunicaţii, stabilește răspunderea pentru încălcarea regulilor de securitate și accesul neautorizat la rețele. Aceste articole subliniază importanța respectării standardelor de securitate în domeniul sănătății digitale, asigurând că datele privind sănătatea sunt stocate și transmise în condiții de maximă siguranță.

De asemenea, în capitolul privind infracţiunile contra drepturilor politice, de muncă şi altor drepturi constituţionale ale cetăţenilor, articolul 177. *Încălcarea inviolabilităţii vieţii personale*, adică culegerea ilegală sau răspîndirea cu bună-ştiinţă a informaţiilor, ocrotite de lege, despre viaţa personală ce constituie secret personal sau familial al altei persoane fără consimţământul ei.

Tot aici menționăm si în privința articolul 213. *Încălcarea din neglijenţă a regulilor şi metodelor de acordare a asistenţei medicale* de către medic sau de către un alt lucrător medical a regulilor sau metodelor de acordare a asistenţei medicale, dacă aceasta a cauzat vătămarea gravă a integrităţii corporale sau a sănătăţii sau decesul pacientului.

Astfel, aceste norme oferă un cadru juridic pentru protejarea datelor despre pacienți și pentru prevenirea infracțiunilor privind utilizarea abuzivă sau accesul la datele referitoare la sănătate. Aceasta reprezintă un element important pentru a menține încrederea în sistemul de sănătate și pentru a asigura confidențialitatea și siguranța pacienților.

Măsurile și strategiile de contracarare pentru protejarea drepturilor pacienților cuprind o gamă largă de măsuri, care includ măsuri legale, tehnologice și organizatorice, a căror evaluare a eficienței este esențială.

Printre măsurile tehnologice se numără în mod proeminent criptarea datelor, autentificarea multi-factor, actualizările periodice ale software-ului și utilizarea firewall-urilor și a programelor antivirus, care s-au dovedit eficiente în prevenirea accesului neautorizat la date și a atacurilor cibernetice.

Formarea personalului în domeniul securității cibernetice și al protecției datelor joacă, de asemenea, un rol esențial în prevenirea cazurilor de divulgare a datelor, prin creșterea gradului de conștientizare a personalului cu privire la potențialele amenințări și prin formarea acestuia pentru a răspunde în mod corespunzător la astfel de incidente. Măsurile juridice, inclusiv legile și reglementările, oferă un cadru legal pentru protecția datelor, ajutând instituțiile să reducă la minimum riscurile și să asigure un nivel adecvat de protecție a datelor.

Implementarea unor proceduri stricte de gestionare a accesului la date și elaborarea unor planuri eficiente de răspuns la incidentele de securitate cibernetică sunt elemente importante ale unei strategii de securitate, care permit de a răspunde rapid la amenințările la adresa securității și de a reduce la minim daunele potențiale. Efectuarea periodică de audituri de securitate și evaluări ale riscurilor ajută la identificarea vulnerabilităților de securitate și la abordarea rapidă a acestora, ceea ce este eficient în prevenirea amenințărilor și asigurarea la standardele de securitate în continuă schimbare.

Utilizarea serviciilor cloud cu niveluri ridicate de securitate și aplicarea inteligenței artificiale și a machine learning pentru a detecta amenințările sporesc, de asemenea, protecția datelor. Dezvoltarea și punerea în aplicare a sistemelor bazate pe inteligență artificială pentru monitorizarea și detectarea tiparelor neobișnuite în traficul de rețea și în comportamentul utilizatorilor permite detectarea și prevenirea în timp real a potențialelor atacuri cibernetice.

Aplicarea combinată a acestor măsuri asigură o protecție a datelor și a drepturilor pacienților pe diferite planuri în domeniul asistenței medicale. În ciuda complexității și dinamismului amenințărilor cibernetice, combinația de strategii tehnologice, organizaționale și juridice asigură în mod eficient securitatea și confidențialitatea în domeniul asistenței medicale.

Concluzii

Tehnologiile digitale au contribuit la îmbunătățirea semnificativă a asistenței medicale, oferind servicii medicale mai accesibile, gestionarea eficientă a datelor și dezvoltarea medicinei individualizate. Cu toate acestea, odată cu apariția lor au apărut noi provocări, inclusiv amenințări la adresa securității cibernetice și a securității datelor, care necesită măsuri de securitate sporite și dezvoltarea cadrului juridic și de reglementare.

Adaptarea la aceste schimbări și protejarea drepturilor și siguranței pacienților necesită o abordare integrată care să includă elaborarea de strategii tehnologice, organizaționale și juridice. Securitatea cibernetică, formarea personalului, sensibilizarea pacienților și respectarea standardelor legale sunt aspecte importante.

Pentru a asigura o asistență medicală sigură și eficientă, respectând în același timp drepturile și viața privată a pacienților, trebuie menținut în viitor un echilibru între inovare și protecția datelor. În acest sens, va fi nevoie de un efort de colaborare

între instituțiile publice, sectorul privat, comunitatea internațională și participarea activă a pacienților.

Propunerile pentru cercetări viitoare în acest domeniu includ examinarea impactului noilor tehnologii, cum ar fi inteligența artificială și machine learning, asupra protecției datelor și a drepturilor pacienților, cu accent pe aspectele etice și juridice. De asemenea, sunt importante analiza noilor metode de protecție a datelor, inclusiv blockchain și tehnici avansate de criptare, evaluarea impactului cooperării internaționale asupra îmbunătățirii securității datelor și examinarea rolului inițiativelor educaționale pentru creșterea gradului de conștientizare în materie de securitate cibernetică. Astfel de studii vor contribui la dezvoltarea unor soluții eficiente pentru protejarea drepturilor și siguranței pacienților în era digitalizării medicinei.

Referințe bibliografice:

1. Грибанов Ю.И. Основные модели создания отраслевых цифровых платформ. In: *Вопросы инновационной экономики,* 2018, Том 8, № 2, С. 223-234. [citat 23.11.2023]. Disponibil: https://cyberleninka.ru/article/n/osnovnye-modeli-sozdaniya-otraslevyh-tsifrovyh-platform/pdf
2. Карцхия А.А. Цифровая медицина - реальность сегодняшнего дня. In: *Экономические и социальные проблемы России,* 2021, № 2, С. 132-142. [citat 23.11.2023]. Disponibil: https://cyberleninka.ru/article/n/tsifrovaya-meditsina-realnost-segodnyashnego-dnya
3. Goldsmith J. Digital medicine: implications for healthcare leaders. Chicago: Health administration press, 2003. 223 p. [citat 23.11.2023]. Disponibil: http://book.itep.ru/depository/it_ med/GS_ DIGITAL_ MED_1199.pdf.
4. Kataria S., Ravindran V. Electronic health records: a critical appraisal of strengths and limitations. In: *J R Coll Physicians Edinb*. 2020 Sep;50(3):262-268. doi: 10.4997/JRCPE.2020.309. PMID: 32936099.
5. Evans R.S. Electronic Health Records: Then, Now, and in the Future. In: *Yearb Med Inform.* 2016 May 20;Suppl 1(Suppl 1):S48-61. doi: 10.15265/IYS-2016-s006. PMID: 27199197; PMCID: PMC5171496.
6. Colbert G.B, Venegas-Vera A.V, Lerma E.V. Utility of telemedicine in the COVID-19 era. In: *Rev Cardiovasc Med.* 2020 Dec 30;21(4):583-587. doi: 10.31083/j.rcm.2020.04.188. PMID: 33388003.
7. Omboni S., Padwal R.S., Alessa T., Benczúr B., Green B.B., et al. The worldwide impact of telemedicine during COVID-19: current evidence and recommendations for the future. In: *Connect Health.* 2022 Jan 4;1:7-35. doi: 10.20517/ch.2021.03. PMID: 35233563; PMCID: PMC7612439.
8. Gajarawala S.N., Pelkowski J.N. Telehealth Benefits and Barriers. *J Nurse Pract.* 2021 Feb;17(2):218-221. doi: 10.1016/j.nurpra.2020.09.013. In*: Epub* 2020 Oct 21. PMID: 33106751; PMCID: PMC7577680.

9. Цыганова О.А., Светличная Т.Г., Трофимов В.В. Анализ международного законодательства, регламентирующего защиту прав пациентов. In: *Экология человека,* №1, 2013. С. 20-24. [citat 23.11.2023]. Disponibil: https://doi.org/10.17816/humeco17391
10. Гафурова Н., Юсупова Ф. Анализ международного законодательства, регулирующего защиту прав пациентов. In: *Азиатско-Тихоокеанский журнал окружающей среды и рака* 2022, Том 5, № 1: Спецвыпуск: Инновационные технологии в медицине. [citat 23.11.2023]. Disponibil: http://waocp.com/journal/index.php/apjec/article/view/1043#sec-0
11. Legea Republicii Moldova cu privire la drepturile şi responsabilităţile pacientului, nr. 263 din 27-10-2005. In: Monitorul Oficial, 30.12.2005, nr. 176-181 art. 867. [citat 23.11.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=129085&lang=ro
12. World Health Organization, WHO Regional Office for Europe. *Declaration on the Promotion of Patients' Rights in Europe*, reprinted in 45 International Digest of Health Legislation 411 (1995). [citat 23.11.2023]. Disponibil: http://hrlibrary.umn.edu/instree/patientrights.html
13. WMA Declaration of Lisbon on the Rights of the Patient. Adopted by the 34th World Medical Assembly, Lisbon, Portugal, September/October 1981. [citat 23.11.2023]. Disponibil: https://www.wma.net/policies-post/wma-declaration-of-lisbon-on-the-rights-of-the-patient/
14. *Status and Rights of Patients*. Issued in Helsinki on 17th August 1992. [citat 23.11.2023]. Disponibil: https://www.finlex.fi/en/laki/kaannokset/1992/en19920785_20120690.pdf
15. *European Charter of Patients' Rights*. Basis document. Rome, November 2002. Preamble. [citat 23.11.2023]. Disponibil: https://ec.europa.eu/health/ph_overview/co_operation/ mobility/docs/ health_services_co108_en.pdf
16. Утечки данных в медицинских учреждениях. ZDRAV.EXPERT, 2023. [citat 23.11.2023]. Disponibil: https://zdrav.expert/index.php/Статья:Утечки_данных_в_медицинских_ учреждениях
17. *Защита персональных данных в медицине: что нужно знать?* Центр безопасности данных. [citat 23.11.2023]. Disponibil: https://data-sec.ru/public/personal-data/zashchita-pdn-v-meditsine/
18. Ghafur S., Kristensen S., Honeyford K., Martin G., Darzi A., Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. In: *NPJ Digit Med.* 2019 Oct 2;2:98. doi: 10.1038/s41746-019-0161-6. PMID: 31602404; PMCID: PMC6775064.
19. Unauthorised Possession and Disclosure of Information from HIV Registry. *Ministry of Health Singapore,* 28th Jan 2019. [citat 23.11.2023]. Disponibil: https://www.moh.gov.sg/news-highlights/details/unauthorised-possession-and-disclosure-of-information-from-hiv-registry

20. MyFitnessPal Account Security Issue: Frequently Asked Questions [citat 23.11.2023]. Disponibil: https://content.myfitnesspal.com/security-information/FAQ.html.
21. Черновицкая Ю.В. Цифровые технологии в медицине: специфика ответственности при их использовании. In: *Научный результат. Социальные и гуманитарные исследования*. 2020. Т. 6, № 4. С. 89-101 doi: 10.18413/2408-932X-2020-6-4-0-10.
22. European Parliament and Council of the European Union. (2018). General Data Protection Regulation (GDPR). In: *Official Journal of the European Union*, L 119/1. [citat 23.11.2023]. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016 R0679
23. U.S. Department of Health & Human Services. (2020). Health Insurance Portability and Accountability Act (HIPAA). In: *Public Law* 104-191. [citat 23.11.2023]. Disponibil: https://www.hhs.gov/hipaa/index.html
24. *Data Protection Act* 1998. [citat 23.11.2023]. Disponibil: http://www. legislation. gov. uk/ukpga/1998/29/ contents.
25. Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». [citat 23.11.2023]. Disponibil: https://www.consultant.ru/document/cons_doc_LAW_618 01/
26. Legea Republicii Moldova privind protecția datelor cu caracter personal, nr. 133 din 08.07.2011. In: Monitorul Oficial al Republicii Moldova, 14.10.2011, nr. 170-175 art. 492. [citat 23.11.2023]. Disponibil: https://www.legis.md/cautare/getResults?doc_id=10607&lang=ro
27. Universal Declaration of Human Rights (UDHR). Proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A). 20.08.2023. [citat 23.11.2023]. Disponibil: https://www.un.org/en/about-us/universal-declaration-of-human-rights
28. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5. [citat 23.11.2023]. Disponibil: https://www.refworld.org/docid/3ae6b3b04.html
29. Cod nr. 985 din 18-04-2002 Codul Penal al Republicii Moldova. Publicat: 14-04-2009 în Monitorul Oficial Nr. 72-74 art. 195. [citat 23.11.2023]. Disponibil: https://www.legis.md/cautare/getResults? doc_id=129474&lang=ro