UNIVERSITATEA „BABEȘ-BOLYAI”
FACULTATEA DE DREPT

PROTEJAREA CIBERNETICĂ A VIEȚII PRIVATE DE CĂTRE INTERMEDIARI

(CUPRINS ȘI REZUMAT)

Coordonator științific :
Prof. Univ. Dr. Vasiu Ioana

Doctorand:

Gabudeanu Larisa

Cluj-Napoca

2024

În ultimele decenii, numărul de servicii online pentru clienți a crescut, precum și numărul de clienți care aleg să obțină servicii online. Pentru consumatori, un număr semnificativ de tranzacții cu produse și servicii sunt efectuate online, prin diverși intermediari. Potrivit unui studiu realizat de Capgemini, la nivel global au fost efectuate aproximativ 1,3 trilioane de tranzacții fără numerar în 2023, de la aproximativ 500 de miliarde în 2018.[1] Mai mult, în ceea ce privește marketingul către consumatori, profilarea consumatorilor în vederea identificării preferințelor lor este larg răspândită și de obicei utilizat pe mai multe platforme.[2] În consecință, persoanele folosesc din ce în ce mai mult resursele de internet.

De asemenea, în ceea ce privește relațiile dintre autorități și cetățeni, au fost realizate diverse proiecte informatice pentru principala interacțiune între cei doi, inclusiv plata taxelor, eliberarea documentelor oficiale, procedurile de achiziții publice, informații fiscale/fiscale, proceduri de contencios, acces electronic la dosare în litigiu și urmărire penală, examinări la nivel național în școli și alegeri în formă electronică. Cel mai bun exemplu în acest sens este Estonia, cu abordarea sa de e-guvernare.[3] Acest lucru a generat, de asemenea, o cantitate mare de date referitoare la persoane, care urmează să fie stocate și prelucrate de autoritățile publice.

În acest scop, accentul acestei teze este rolul intermediarilor (definiți ca sisteme de operare, browsere, aplicații stocate și hardware) în asigurarea măsurilor de prevenire în vigoare pentru a proteja persoanele. Am ales acest punct de vedere, deoarece intermediarii sunt cei mai bine plasați pentru a îmbunătăți cerințele legale privind măsurile preventive existente, având în vedere accesul lor unic la date și posibilitatea de interacțiune cu persoanele. În ceea ce privește obiectivele acestei teze, ne concentrăm mai întâi pe identificarea intruzivității în contextul asigurării securității persoanelor. În acest scop, am inclus o analiză a limitărilor privind luarea automată a deciziilor în scopuri de securitate, utilizarea mecanismelor de apărare active, precum și protecția datelor și limitările din dreptul penal la colectarea datelor, agregarea datelor și partajarea datelor cu autoritățile și entitățile private. Acest lucru este corelat pe tot parcursul tezei cu constrângerile tehnice ale intermediarilor în ceea ce privește identificarea amenințărilor cibernetice sau a atacurilor cibernetice sau în ceea ce privește prevenirea acestora. Acest lucru este extrem de relevant în ceea ce privește stabilirea unor roluri și responsabilități adecvate în cadrul ecosistemului digital care reflectă scenariile tehnice din viața reală. O schiță a obiectivelor este inclusă mai jos:

Obiectivul 1: Stabilirea criteriilor de identificare a intruzivității în contextul asigurării securității persoanelor. Aceasta ia în considerare datele colectate, datele agregate (profilare), datele dezvăluite și notificări, împreună cu modificările care urmează a fi aduse legislației penale și legislației privind protecția datelor.

---

[1] Capgemeni , Global non-cash transaction vulumes , 2023, https://www.capgemini.com/news/press-releases/global-non-cash-transaction-volumes-set-to-reach-1-3-trillion-in -2023/ , ultima accesare la 16 octombrie 2023. Capgemini și BNPP, 2018 World Payments Report, https://www.worldpaymentsreport.com, ultima accesare la 28 decembrie 2022.

[2]Cercetările Parker, Clifton, New Stanford arată că computerele sunt mai bune judecători de personalitate decât prietenii și familia, 2015, https://news.stanford.edu/2015/01/12/personality-computer-knows-011215/ , ultima accesare pe 24 decembrie 2022.

[3]INSEAD/WIPO, 2017 report - Global Innovation Index 2017 Report, https://www.globalinnovationindex.org/gii-2017-report , ultima accesare la 28 decembrie 2022. WIPO, Global Innovation Index, 2023, https://www. wipo.int/edocs/pubdocs/en/wipo-pub-2000-2023-en-main-report-global-innovation-index-2023-16th-edition.pdf, ultima accesare la 21 octombrie 2023.

Subobiectiv 1.1: Identificarea limitelor măsurilor de securitate prin implementarea minimizării datelor (inclusiv în agregarea datelor și partajarea datelor) și a cerințelor de luare a deciziilor automatizate de protecție a datelor.

Subobiectiv 1.2: Posibilitatea de a utiliza anumite tipuri de apărare activă în conformitate cu legislația existentă și propunerea de modificări ale legislației privind protecția datelor și legislația penală pentru a le adapta și partajarea datelor cu alți intermediari sau alte entități.

Obiectivul 2: Identificarea rolului care urmează să fie definit pentru intermediari (sisteme de operare, furnizori de hardware, browsere, magazine de aplicații) în ceea ce privește asigurarea securității, echilibrând totodată confidențialitatea (inclusiv lipsa de intruzivă).

Subobiectiv 2.1: Modificări care sunt necesare la legislația existentă pentru a asigura responsabilitatea acestor intermediari, deoarece rolul și obligațiile lor nu sunt acoperite pe deplin de legislația existentă prin referire la implicarea în viața reală a acestor intermediari în prelucrarea datelor persoanelor fizice.

Subobiectiv 2.2: Modificări propuse la legislația existentă privind protecția datelor și legislația penală în vederea asigurării posibilității măsurilor de securitate asigurate de intermediari și, în același timp, a limitelor tipurilor de măsuri de securitate care pot fi luate, având în vedere legislația și limitări tehnice în acest sens.

Rezultatul analizei include lacune identificate în legislația penală actuală și legislația aferentă, împreună cu propuneri legislative pentru instituirea unor cerințe legale relevante pentru rolul intermediarilor în prevenirea încălcărilor vieții private a persoanelor fizice. Principalele rezultate care constituie o noutate adusă de această teză includ următoarele aspecte:

- Propunere de îmbunătățire a conceptului de viață privată în vederea reflectării datelor digitale stocate și utilizate de persoane și a riscului asociat cu acestea.
- Noi obligații pentru intermediari în ceea ce privește prevenirea amenințărilor cibernetice și a atacurilor cibernetice, prin referire la datele la care au acces, posibilitatea de a interacționa cu persoanele fizice/utilizatorii (și cu autoritățile și alte entități private), dar și prin referire la limitările tehnice și operaționale în identificarea sau abordarea amenințărilor cibernetice și a atacurilor cibernetice.
- Reglementarea abordării bazate pe risc a obligațiilor intermediarilor și, prin urmare, analiza corelată a abordării bazate pe riscuri de avut în vedere la stabilirea răspunderii penale.
- Implicarea și răspunderea utilizatorului în anumite cazuri de utilizare limitată în care este necesară contribuția sau acțiunea sa și în caz de inacțiune/acțiune cu intenție.
- Posibilitatea intermediarilor de a stabili mecanisme active de apărare și nivelul de acțiuni care pot fi întreprinse având în vedere implicațiile de drept penal ale unor astfel de acțiuni.
- Posibilitatea extinderii măsurii de autoapărare pentru acțiunile efectuate de intermediari în numele utilizatorului.
- Limitări legale privind agregarea datelor de la mai mulți utilizatori și cerințele pentru anonimizarea acestora.

- Mecanism de cooperare între intermediari și autorități sau alte părți interesate digitale, cu respectarea legislației penale existente și a limitărilor privind protecția datelor.

În ceea ce privește metodologia cercetării, în primul rând, am realizat o analiză și o comparație a principalelor caracteristici ale intruzivității în dreptul penal și jurisprudența privind protecția datelor și sancțiunile privind protecția datelor în UE (legislație, jurisprudență și orientări de implementare în dreptul penal, drepturile omului și domenii de protecție a datelor). În al doilea rând, am efectuat o analiză a echilibrului dintre securitate și confidențialitate în doctrina juridică, jurisprudență și sancțiunile privind protecția datelor la nivel de legislație europeană și românească în ceea ce privește legislația în vigoare în prezent și proiecte de propuneri, împreună cu cele mai bune practici din SUA conturate în legislație. doctrină și relevante pentru sistemul juridic al UE.

Prin aceste două metode am identificat rolul intermediarilor în legislația actuală a UE și orice limitări în ceea ce privește implementarea unei obligații pentru intermediari de a asigura măsuri preventive de securitate adecvate. Având în vedere aplicabilitatea practică a obiectivelor și ipotezei, am făcut o comparație între multiplele politici/funcții de confidențialitate și securitate ale intermediarilor – cel puțin 3 din fiecare categorie – sistem de operare, browser și furnizor de magazin de aplicații pe un anumit set de criterii pentru a identifica modul în care abordează în prezent măsurile preventive pentru securitatea vieții private a utilizatorilor lor. În plus, pentru rezultatele analizei de mai sus, am inclus o validare a lacunelor identificate în legislație, limitări de natură juridică și tehnică în asigurarea securității corespunzătoare a vieții private a persoanelor fizice prin chestionar cantitativ pe persoane fizice (utilizatori finali), consilieri juridici. și experți IT. Rezultatele și concluziile din chestionar sunt incluse la sfârșitul fiecărei secțiuni din teză.

Conceptul de viață privată a apărut în termeni de legislație europeană de la convențiile privind drepturile omului la legislația privind protecția datelor și la convențiile de drept penal. Cu toate acestea, acest concept și protecția sa au fost avute în vedere mai mult în ceea ce privește peisajul fizic și limitat în ceea ce privește peisajul digital, așa cum se arată în acest capitol și în titlul II de mai jos. Am identificat anumite limitări în definirea infracțiunii de încălcare a vieții private în legislația la nivelul UE și la[4] nivelul legislației române prin referire la lumea digitală în schimbare în care viața privată este din ce în ce mai digitalizată în raport cu anumiți intermediari: sistemul de operare, browser, magazin de aplicații și furnizor de hardware. După cum se detaliază mai jos, există o lipsă a cerințelor legale adecvate pentru măsurile de securitate pentru prevenirea încălcării vieții private, astfel de cerințe legale fiind aplicabile pentru o categorie de părți interesate din ecosistemul digital, respectiv, intermediarii menționați mai sus. [5]

Tipurile de date analizate în această teză includ date stocate pe dispozitivul utilizatorului și pe serverul serviciului online utilizat de utilizator (inclusiv serverele subcontractanților furnizorului de servicii online).[6] Datele includ tipuri de date structurate și nestructurate care se referă la conținutul creat, încărcat sau primit de utilizator și interacțiunea

---

[4] Slavoiu , Radu, Protectia penala a vietii private, Universul Juridic, pag . 152, 2016

[5]Gasser, U. și Schulz, W. Guvernarea intermediarilor online: Observații dintr-o serie de studii de caz naționale. Seria de publicații Centrul Berkman pentru Internet și Societate de la Universitatea Harvard , nr. 2015-5. Boston. http://dx.doi.org/10.2139/ssrn.2566364, ultima accesare pe 8 decembrie 2022.

[6]Acharya, S.; Rawat, U.; Bhatnagar, R. O revizuire cuprinzătoare a securității Android: amenințări, vulnerabilități, detectarea programelor malware și analiză. Securizat . Comun . Netw . 2022.

utilizatorului cu dispozitivul, serviciul online sau mediul și datele referitoare la autorii (potențialii) autori sau în legătură cu IT sistemele utilizate de făptuitori.[7] Teza aduce perspective suplimentare în extinderea definiției vieții private pentru a se adapta utilizării curente a dispozitivelor digitale și a datelor într-o lume interconectată.

De asemenea, teza subliniază nevoia de claritate suplimentară în cazul în care intermediarii sunt utilizați pentru astfel de activități. Acest lucru implică, de asemenea, mecanismele de cooperare existente și care trebuiau instituite în vederea cooperării cu alte entități și autorități private (fie autoritățile de anchetă penală, fie autoritățile de securitate cibernetică). Articolul 29 din Grupul de lucru[8] a subliniat, de asemenea, necesitatea de a aborda rolul intermediarilor online prin referire la rolul tehnic și economic al fiecărui tip de astfel de intermediari. Intermediarii precum sistemele de operare, browserele și furnizorii de hardware sunt cei care interacționează cel mai mult cu indivizii online și au cea mai largă imagine de ansamblu asupra activității individului online.[9]

Având în vedere contextul legislativ menționat mai sus, există două unghiuri care necesită cercetări și clarificări suplimentare. Una era legată de utilitatea profilării și monitorizării utilizatorilor pentru a asigura măsuri de securitate adecvate,[10] iar cealaltă de necesitatea de a partaja date între diverși părți interesate din aceeași industrie sau între industrii pentru a asigura implementarea măsurilor de securitate preventive adecvate înainte de apariția securității. incidente.[11]

În plus, în ceea ce privește măsurile preventive pentru protecția vieții private, în contextul peisajului digital există cerințe legale limitate în acest sens, după cum se detaliază mai jos. Această teză identifică lipsa unor prevederi legale care să stabilească clar nivelul măsurilor de securitate care ar trebui implementate de către entitățile private pentru a asigura protecția drepturilor la viață privată.[12] Aceasta include, de asemenea, implicarea terților în stabilirea și stabilirea măsurilor de securitate preventivă. În plus, teza conturează îmbunătățiri propuse pentru clarificarea rolului fiecărei părți interesate și limitările obligațiilor privind măsurile de securitate.[13]

Având în vedere noile unghiuri de analiză de mai sus a cerințelor legale existente, această teză deschide discuțiile cu privire la câteva puncte în care există o intersecție între

---

[7]Maimon, David, Louderback, Eric R., Cyber-dependent crimes: An interdisciplinary review, Annual Review of Criminology 2, pp. 191-216, 2019.

[8]Grupul de lucru Articolul 29, Document de lucru, Confidențialitatea pe Internet – O abordare integrată a UE pentru protecția datelor online, 2000.

[9]Tribunalul Timis, decizia nr. 166/2017 privind potențiala răspundere a proprietarului unui centru de date pentru activități ilegale desfășurate folosind serverele din centrul de date .

[10]Schiopu, Silviu-Dorin, Privire generală asupra măsurilor tehnice si organizatorice necesare pentru zona de implementare efectivă a Regulamentului general privind protectia date , Revista Romana de Drept al Afacerilor 2/2019, 2019.

[11]Grupul de Cooperare INS, Document de referință privind măsurile de securitate pentru Operatorii Serviciilor Esențiale, Publicația CG 01/2018, 2018.

[12]ENISA, Proactive Detection of Security Incidents, 2012. Ioana, Martin, Detectarea proactive a atacurilor cibernetice – honeypot-urile, Revista de investigare a criminalitatii , suppl. Numărul special 1; Bucuresti vol. 8, nr . 1, p. 151-157, 2015.

[13]Moore R., The Case for Regulating Quality in Computer Security Applications, în Jurnalul European de Drept și Tehnologie, vol. 4, nr. 3, 2013. Kristin E. Heckman et al., Cyber Denial, Deception and Counter Deception A Framework for Supporting Active Cyber Defense , 2015. Arthur Cockfield, Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance, 29 Queen's Law Journal, pp. 364-407, 2003.

protecția datelor și prevederile legale de drept penal.[14] În plus, cercetarea scoate la lumină problemele care apar din aspectele tehnice ale amenințărilor cibernetice și ale mecanismelor de prevenire a securității cibernetice, împreună cu limitările acestora. Există o linie foarte subțire între acțiunile pe care o companie le poate întreprinde pentru a-și proteja datele și încălcarea drepturilor altor persoane (de exemplu, făptuitorii, deținătorii de sisteme informatice utilizate în timpul săvârșirii unei infracțiuni).[15]

Scopul acestei teze este de a analiza această linie subțire și de a determina situațiile care constituie o modalitate legitimă de asigurare a măsurilor de securitate, împreună cu propuneri de modificări în legislație sau în interpretare (în funcție de oportunitatea economică și tehnică a unor astfel de modificări). Având în vedere formularea generală a legislației de implementare a măsurilor de securitate, implementarea acesteia în practică a evoluat în principal pe baza practicii și standardelor sectorului privat. În plus, există o interacțiune între cerințele legale în ceea ce privește securitatea (de exemplu, Directiva NIS, legislația bancară, GDPR)[16] și în ceea ce privește protecția vieții private (ex. CEDO, GDPR, Convenția de la Budapesta privind criminalitatea cibernetică, Codul penal român).

Această teză aduce o nouă lumină asupra obligației de a asigura măsuri tehnice și organizatorice de securitate preventivă, întrucât analizează limitările apărării active de obicei cercetate și ale partajării datelor bazate pe protecția datelor și obligațiile de drept penal.[17] Chiar dacă nu este reglementată în mod expres ca măsură de securitate, strângerea de informații despre tiparele și autorii de atacuri cibernetice existente este o informație utilă pentru structurarea unui sistem IT rezistent într-o entitate privată.[18]

Titlul II se referă la încadrarea contextului vieții private și a rolului intruziv din perspectiva penală, a protecției datelor și a drepturilor omului în vederea consolidării contextului actual al legislației penale.[19] Capitolul II.1 analizează conceptul de viață privată și de intruzivă în cadrul diferitelor tipuri de legislație. În acest scop, în capitolul II.2 există și o analiză a implicațiilor intruzive asupra vieții private în contextul profilării și luării deciziilor automatizate, care este unul dintre cele mai esențiale aspecte având în vedere ecosistemul digital și dependența acestuia de procesarea unor cantități mari. de date și furnizarea de răspunsuri în timp real.[20] În plus, capitolul II.3 trece în revistă modul în care anumite capacități tehnice în ceea ce privește utilizarea honeypot-urilor și a mecanismelor active de apărare pot fi utilizate pentru a asigura prevenirea adecvată a atacurilor cibernetice, recuperarea datelor furate (sau ștergerea acestora) și reținerea autor.

---

[14]Walters, Robert, Novak, Marko, Securitate cibernetică, Inteligență artificială, Protecția datelor și legea, Springer, 2021.

[15]Maimon, David și Eric R. Louderback, Cyber-dependent crimes: An interdisciplinary review, Annual Review of Criminology 2, pp. 191-216, 2019.

[16] Schünemann , W., Baumann, MO, Confidențialitate, protecție a datelor și securitate cibernetică în Europa, Springer, 2017.

[17]Hathaway, Oona și colab., The Law of Cyber-Attack, California Law Review 100(4), 2011.

[18]Cheng, B.; Kikuta, T.; Toshimitsu, Y.; Saito, T. Investigarea atacului asupra consumului de energie pe dispozitivele Android. În Proceedings of the International Conference on Advanced Information Networking and Applications, Toronto, ON, Canada, 12–14 mai 2021; Springer: Berlin/Heidelberg, Germania, pp. 567–579, 2021.

[19]Ho, Heemeng , Ko, Ryan, Mazerolle, Lorraine, Tehnici situaționale de prevenire a criminalității (SCP) pentru prevenirea și controlul infracțiunilor cibernetice: o revizuire sistematică concentrată, Computere și securitate, vol. 115, 2022, https://doi.org/10.1016/j.cose.2022.102611.

[20]Schmitt, Julia, Miller, Klaus M., Skiera, Bernd, The impact of privacy laws on online user behavior , Document de lucru, Universitatea Goethe Frankfurt, HEC Paris, 2020.

Capitolul II.1 se concentrează pe subobiectivul 1.1 și pe ipoteza 1.1.1 în vederea identificării conceptului de intruzivitate și a modului în care acesta se leagă de viața privată în vederea propunerii unei îmbunătățiri a conceptului de viață privată existent în cadrul infracțiunii de viață privată în Codul penal român.[21] În acest scop, capitolul începe cu Secțiunea II.1.1 concentrându-se pe conceptele de intruzivitate și viață privată, continuă cu datele acoperite de conceptul de viață privată din Secțiunea II.1.2 și include prejudiciile legate de confidențialitate care trebuie avute în vedere pentru analiza încălcării vieții private în secțiunea II.1.4, în timp ce secțiunea II.1.5 se concentrează pe localizarea acestor date sau a utilizatorului în vederea determinării impactului acestora asupra protecției vieții private.[22] Rolul consimțământului este deosebit de important în acest context, deoarece este una dintre principalele moduri în care au loc anumite încălcări ale vieții private și acest lucru este analizat în Secțiunea II.1.4.[23]

Capitolul II.2 se referă la subobiectivul 1.1 care se referă la ipoteza 1.1.2, întrucât mecanismele de prevenire, pentru a fi eficiente, presupun automatizarea și agregarea datelor. Astfel de aspecte au anumite limitări legale în legislația actuală.[24] Cu toate acestea, există anumite puncte care încă nu sunt pe deplin abordate și care necesită prevederi legale suplimentare. Capitolul abordează, de asemenea, ipoteza 1.1.3, care este legată de anonimizare/pseudonimizare și necesitatea unei reglementări legale ulterioare în acest sens în ceea ce privește utilizarea tehnicilor de anonimizare/pseudonimizare pentru luarea automată a deciziilor în contextul măsurilor de securitate.[25]

Luarea automată a deciziilor nu implică automat utilizarea învățării automate sau a inteligenței artificiale. Cu toate acestea, acesta este în general cazul în starea actuală a măsurilor de securitate.[26] Secțiunile din acest capitol includ mai întâi aspectele tehnice ale procesului decizional automatizat legate de orice implicații juridice (Secțiunea II.2.1). Ulterior, intră în joc opțiunile de luare a deciziilor (Secțiunea II.2.2), acestea fiind cele care produc efecte juridice asupra persoanelor ale căror date au fost colectate și prelucrate.

Implicarea altor entități în procesul decizional și/sau implementarea deciziilor este inclusă în Secțiunea II.2.3. Implicațiile juridice ale utilizării procesului decizional automat sunt analizate în continuare și propuneri de modificări sunt făcute în Secțiunea II.2.4. Tehnicile de anonimizare/pseudonimizare și implicațiile lor juridice și tehnice sunt incluse în Secțiunea II.2.5.

Capitolul II.3 se adresează subobiectivului 1.2, întrucât se referă la mecanismele active

---

[21]Robinson, L., şi colab. Digital Inequalities 3.0: Emergent Inegalities in the Information Age, Prima luni, vol. 25, nr. 7, Bibliotecile Universității din Illinois, 2020.

[22]Devlin, MA, Hayes, BP, Non-Intrusive Load Monitoring and Classification of Activities of Daily Living Using Residential Smart Meter Data, IEEE Transactions on Consumer Electronics, vol. 65, nr. 3, p. 339-348, aug. 2019, doi : 10.1109/TCE.2019.2918922.

[23]Solove, Daniel J., Murky Consent: An Approach to the Fictions of Consent in Privacy Law, 104 Boston University Law Review (următor), GWU Legal Studies Thesis No. 2023-23, GWU Law School Public Law Thesis No. 2023-23 , 2023, https://ssrn.com/abstract=4333743 sau http://dx.doi.org/10.2139/ssrn.4333743.

[24]Moss, Emanuel, Watkins, Elizabeth, Singh, Ranjit, Elish, Madeleine Clare, Metcalf, Jacob, Assembling Accountability: Algorithmic Impact Assessment for the Public Interest, 2021, https://ssrn.com/abstract=3877437, ultima accesare pe 28 august 2023.

[25]Hongbin, F., Zhi, Z. Schemă de agregare a datelor pentru păstrarea confidențialității, bazată pe învățarea federată pentru IIoT . Matematică, voi. 11, pag . 214, 2023. https://doi.org/10.3390/math11010214

[26]Gibert, D., Mateu, C., Planes, J., The rise of machine learning for detecting and classification of malware: Research developments, trends and challenges. J. Netw . Calculați . Apl., voi. 153, 102526, 2020.

de apărare care pot fi preluate de intermediar.[27] Există anumite acțiuni tehnice care pot fi întreprinse de intermediar în această etapă.[28] Cu toate acestea, în conformitate cu legislația actuală, în special cea privind protecția datelor și legislația penală, există anumite limitări în acest sens.[29] Tipurile de acțiuni care pot fi întreprinse din perspectivă tehnică și limitările din perspectivă juridică sunt analizate în acest capitol, împreună cu tehnici de anonimizare care pot atenua anumite preocupări și riscuri juridice.[30]

Ipoteza 1.2.1 se referă la posibilitatea intermediarilor de a lua anumiți pași activi în momentul în care este identificată o potențială încălcare a vieții private.[31] O abordare este de a considera aceste acțiuni ca parte a măsurilor de autoapărare luate de intermediari în numele victimei (ipoteza 1.2.3). În plus, după luarea măsurilor active, se obțin anumite date referitoare la potențialul atacator cibernetic și există anumite limitări în ceea ce privește analiza acestor date, partajarea acestora cu alte entități private și partajarea acestora cu autoritățile publice (organisme de reglementare sau de urmărire penală). Mai mult, anumite limitări în ceea ce privește interesul public în vederea menținerii ordinii în ceea ce privește entitățile care au competențe de investigare.

Titlul III cuprinde analiza obligațiilor existente în ceea ce privește protecția vieții private care revin intermediarilor. Acesta include, în general, aspecte legate de subobiectivul 2.1, în sensul propunerii unei noi legislații pentru măsurile preventive adecvate care trebuie luate de intermediari pentru a asigura securitatea vieții private a utilizatorilor acestora. O astfel de protecție se referă și la protecția dispozitivelor și la protecția datelor, deoarece, în mediul digital, acestea sunt interconectate.[32] Prin urmare, infracțiunea de acces ilegal la sistemele informatice este strâns legată de infracțiunea de încălcare a vieții private.[33] Mai mult, titlul include și nevoile de cooperare pentru a obține o securitate preventivă adecvată într-un ecosistem globalizat interconectat, în care informațiile despre amenințări sunt esențiale. În acest sens, o schiță a principalelor părți interesate este esențială.[34]

Cei trei piloni principali ai obligațiilor intermediarilor presupun: obligații legale legate de colectarea și prelucrarea datelor referitoare la utilizatori, aspecte de analizat în ceea ce privește agregarea și partajarea datelor și modalitatea de determinare a răspunderii intermediarilor în mod corespunzător.[35] Acești trei piloni reprezintă principalele puncte de vedere care trebuie luate în considerare pentru analiza obligațiilor existente și necesitatea unor

---

[27]Van Dijck, J., Guvernarea societăților digitale: platforme private, valori publice. Computer Law and Security Review, 36, p.105377, 2020.

[28]Rappaport, John, Some Doubts About 'Democratizing' Criminal Justice, The University of Chicago Law Review, vol. 87, nr. 3, pp. 711–814, 2020, JSTOR, https://www.jstor.org/stable/26910603. Accesat 28 august 2023.

[29] Cioclei , V., Drept penal, Partea speciala I, ed. a III-a, ed. C. H. Beck , pag. 64, 2018.

[30]Hathaway, Oona și colab., The Law of Cyber-Attack, California Law Review 100(4), 2011.

[31]Denning, Dorothy E., Cadrul și principiile pentru apărarea cibernetică activă , Computere și securitate, voi. 40, p. 108-113, 2014, https://doi.org/10.1016/j.cose.2013.11.004.

[32]Losavio, MM, Chow, KP, Koltay, A, James, J., Internetul lucrurilor și orașul inteligent: provocări legale cu criminalistica digitală, confidențialitate și securitate, Jurnalul de securitate și confidențialitate. 2018.

[33]Zhou, G., Zhuge, J., Fan, Y. și colab. O piață în vis: dezvoltarea rapidă a criminalității cibernetice anonime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

[34]Rana, Muhammad Usman, Ellahi, Osama, Alam, Masoom, Webber, Julian L., Mehbodniya , Abolfazl, Khan, Shawal, Offensive Security: Cyber Threat Intelligence Enrichment With Counterintelligence and Counteratack, IEEE Access, vol.10, pp.108760 108774, 2022.

[35]Cowls, Josh, Morley, Jessica, Floridi , Luciano, Guvernarea magazinului de aplicații: Implicații, limitări și răspunsuri de reglementare, Politica de telecomunicații, vol. 47, numărul 1, 2023, https://doi.org/10.1016/j.telpol.2022.102460.

noi obligații suplimentare, în timp ce următorul capitol IV va analiza limitările legislației existente pentru implementarea corectă a acestor obligații.

Capitolul III.1 se concentrează pe obligațiile care sunt în vigoare în prezent și pe cele care pot fi stabilite pentru intermediari, pe baza rolului acestora, așa cum este analizat și detaliat în prezenta teză.[36] În acest scop, capitolul analizează cerințele de securitate pentru colectarea datelor, obligațiile privind asigurarea cerințelor de securitate și tipurile de atac cibernetic care pot fi identificate și analizate de intermediari. În plus, analizează în cooperare cu alte entități din ecosistemul digital și corelarea cu alte infracțiuni relevante în temeiul cărora acțiunile intermediarilor pot fi considerate acțiuni penale, dacă nu este instituită o legislație specifică.[37]Aceasta presupune că trebuie luate măsuri legislative suplimentare pentru ca acțiunile de securitate preventivă ale intermediarilor să nu fie considerate infracțiuni în sine, în special în ceea ce privește încălcarea vieții private a utilizatorilor pe care îi protejează de atacuri cibernetice.[38] Acest capitol include și o privire de ansamblu asupra politicilor și procedurilor făcute publice de intermediari în ceea ce privește măsurile de securitate pe care le-au implementat în temeiul legislației în vigoare și fără cerințe legale specifice în acest sens, dar în vederea protejării cât mai mult posibil a utilizatorilor acestora.[39]

Capitolul III.2 se concentrează asupra modului de implementare a obligației intermediarilor propuse în prezenta teză de a asigura măsuri preventive adecvate. Capitolul analizează modul în care intermediarii pot agrega datele și le pot partaja pentru a le îmbunătăți acuratețea identificării atacurilor cibernetice, a tiparelor de atac cibernetic și a vulnerabilităților exploatabile și a configurărilor greșite exploatabile.[40] În acest scop, capitolul include aspecte legate de partajarea datelor brute sau a rezultatelor analizei de către intermediari către alte entități (inclusiv alți intermediari și autorități), precum și agregarea datelor la nivelul utilizatorului sau la nivelul tuturor utilizatorilor de intermediarul.[41] În plus, utilitatea anonimizării și pseudonimizării este inclusă în acest capitol ca modalitate de a respecta protecția datelor și legislația penală, precum și de asigurare a securității datelor colectate.

Capitolul III.3 include detalii privind modul de stabilire a răspunderii intermediarilor.[42] Include aspecte legate de responsabilitate în legislația actuală privind protecția datelor, drepturile omului și penală și analizează în continuare preocupările juridice pe baza tipurilor de atacuri și a tipului de răspuns la astfel de atacuri.[43] Răspunderea intermediarilor este analizată în continuare în ceea ce privește revizuirea periodică a activității intermediarului,

---

[36]Pistor, Katharina, Rule by Data: The End of Markets?, 83 Law and Contemporary Problems, pp. 101-124, 2020.
[37]Gasser, Urs și Schulz, Wolfgang, Guvernarea intermediarilor online: Observații dintr-o serie de studii de caz naționale, 2015. Publicația de cercetare Berkman Center nr. 2015-5, https://ssrn.com/abstract=2566364 sau http://dx.doi.org/10.2139/ssrn.2566364.
[38]Daniel, LE, Criminalistică digitală pentru profesioniștii în drept. Înțelegerea probelor digitale de la mandatul către sala de judecată, ed. I, ed. Syngress, pag . 124, 2011.
[39]Gasser U, Schulz W., Governance of Online Intermediaries – Observations From a Series of National Case, 2015, https://ssrn.com/abstract=2566364, ultima accesare la 29 august 2023.
[40]Moura, José, Serrão , Carlos, Probleme de securitate și confidențialitate ale datelor mari, parte a Manualului de cercetare privind tendințele și direcțiile viitoare în date mari și inteligență web, 2015.
[41]Corwin, EH. Inspecția profundă a pachetelor: modelarea internetului și implicațiile asupra confidențialității și securității, Jurnalul de securitate a informațiilor: o perspectivă globală, vol. 20(6):311-6., 2011.
[42]Shi, L, Li, K. Sistemul de protecție a confidențialității și de detectare a intruziunilor a rețelei de senzori fără fir bazat pe rețeaua neuronală artificială, Computer Intelligence Neuroscience, voi. 2022:1795454, 2022, doi : 10.1155/2022/1795454.
[43]Alotaibi, Saud, et al., O nouă abordare de profilare a comportamentului pentru autentificarea continuă pentru aplicații mobile, SCITEPRESS-Science and Technology Publications, 2019.

implementarea la timp a măsurilor de securitate și documentarea adecvată a măsurilor de securitate luate și motivarea alegerii acestor măsuri de securitate.

Capitolul III.1 analizează obligațiile actuale din legislația română care pot conduce la interpretarea conform căreia intermediarii au obligații de a păzi viața privată a utilizatorilor și propuneri de ajustare a acestor obligații pentru a reflecta rolul actual al entităților în cadrul ecosistemului digital.[44] Intermediarii sunt poziționați într-o manieră în centrul majorității activităților desfășurate de utilizatori pe dispozitivele lor, având o imagine de ansamblu asupra întregului ecosistem de aplicații și destinații de internet utilizate de utilizatori.[45]

Conform legislației actuale, așa cum se arată în această cercetare, nu există obligații legale de implementare a măsurilor de securitate preventivă.[46] Deși există obligații pentru anumite entități de a implementa anumite măsuri preventive de securitate în cadrul organizației lor sau în cadrul software-ului pe care îl furnizează clienților, intermediarii nu sunt acoperiți de astfel de obligații și, în plus, abordarea de detectare și prevenire a intruziunilor analizată în această teză nu este acoperită la capitolul legislatia existenta. Capitolul se concentrează pe subobiectivul 2.1, respectiv, ipoteza 2.1.1 care se referă la necesitatea unor obligații legale suplimentare ale intermediarilor în vederea prevenirii încălcării vieții, întrucât acest termen a fost definit în legislația în vigoare și modificările propuse menționate în Titlul II de mai sus.

Astfel, acest capitol subliniază indirect utilitatea adăugării unor ajustări de drept penal la conceptul de viață privată, pentru a reflecta peisajul digital. Acest lucru ar aduce conceptul de viață privată și modalitatea de protecție a dreptului penal în conformitate cu digitalizarea care acoperă în prezent activitățile și viața utilizatorilor.[47] În plus, în caz de inacțiune cu intenția de a asigura măsurile de securitate adecvate, ar trebui să fie declanșată o răspundere penală similară, deoarece ajută indirect făptuitorii să comită infracțiunea de încălcare a vieții private.[48] Aceasta presupune că, chiar și sub protecția actuală a vieții private, obligațiile intermediarilor propuse în prezenta teză sunt de fapt solicitate, întrucât orice inactivitate în acest sens poate duce la încălcarea vieții private a utilizatorilor.[49]

Alte două subobiective sunt abordate în acest capitol în ceea ce privește cooperarea, subobiectivul 2.2, cu ipoteza 2.2.3 (limitări tehnice pentru implementarea măsurilor de securitate care sunt dependente de alte entități) și ipoteza 2.1.3 (cooperarea între părțile

---

[44]Declarația Comitetului Miniștrilor privind riscurile la adresa drepturilor fundamentale care decurg din urmărirea digitală și alte tehnologii de supraveghere (adoptată de Comitetul Miniștrilor la 11 iunie 2013 la cea de-a 1173-a reuniune a adjuncților miniștrilor).

[45]Zhang, Lei, Yang, Zhemin , He, Yuyu , Li, Mingqi , Yang, Sen, Yang, Min, Zhang, Yuan, Qian, Zhiyun , Aplicația la mijloc: Demystify Application Virtualization în Android și amenințările sale de securitate. Proc. ACM Măs. Anal. Calculați . Syst. 3, 1, articolul 17, 2019, https://doi.org/10.1145/3322205.3311088.

[46]Harkin, D., Molnar, A., Operating-System Design and Its Implications for Victims of Family Violence: The Comparative Threat of Smart Phone Spyware for Android Versus iPhone Users. Violența împotriva femeilor, vol. 27(6–7), p. 851–875, 2021. https://doi.org/10.1177/1077801220923731.

[47]Zhou, G., Zhuge, J., Fan, Y. și colab. O piață în vis: dezvoltarea rapidă a criminalității cibernetice anonime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

[48]Almomani, IM, Khayer , AA, A Comprehensive Analysis of the Android Permissions System, în IEEE Access, vol. 8, p. 216671-216688, 2020, doi : 10.1109/ACCESS.2020.3041432.

[49]Zhou, G., Zhuge, J., Fan, Y. și colab. O piață în vis: dezvoltarea rapidă a criminalității cibernetice anonime. Mobile Netw Appl 25, pp. 259–270, 2020, https://doi.org/10.1007/s11036-019-01440-2.

interesate digitale pentru asigura implementarea rapidă și eficientă a măsurilor de securitate preventivă).[50]

Capitolul se concentrează mai întâi pe temeiul legal și cerințele legale pentru colectarea datelor despre utilizator.[51] Aceasta implică o privire de ansamblu asupra aspectelor legate de protecția datelor și de dreptul penal. În plus, astfel de cerințe sunt plasate în ecosistemul legislației digitale și în alte infracțiuni reglementate de legea penală decât încălcarea vieții private care poate fi relevantă în mediul digital și pentru protecția vieții private a utilizatorilor.[52] În plus, din perspectivă tehnică practică, cerințele identificate în capitol sunt corelate cu tipurile de atacuri care urmează să fie identificate și analizate de către intermediari și corelarea din perspectivă tehnică cu ceilalți părți interesate din ecosistemul digital.[53] Capitolul include, de asemenea, un studiu de caz pentru a analiza modul în care un set de intermediari gestionează securitatea utilizatorilor lor în prezent, prin referire la obligațiile pe care și le asumă în termenii și condițiile disponibile publicului.[54]

Capitolul III.2 analizează una dintre cele mai importante activități în ceea ce privește prevenirea securității, respectiv, colectarea și analiza datelor de la mai mulți utilizatori și în contextul agregării datelor. Colectarea poate fi efectuată chiar de intermediar sau de la alți intermediari sau terți. Capitolul include analize din multiple perspective legislative și practice, inclusiv protecția datelor și dreptul penal.[55]

Abordările care pot fi luate în practică includ agregarea datelor de la mai multe dispozitive și mai mulți utilizatori. Aceasta oferă o imagine de ansamblu asupra tipologiilor atacatorilor cibernetici și oferă mai multe informații despre vectorii de atac utilizați, în special pentru link-urile rău intenționate trimise în chat-uri și încercări de phishing/vishing. [56]Datele agregate asigură, dintr-o perspectivă statistică și probabilă, o viziune mai precisă asupra peisajului utilizatorilor și asupra amenințărilor cibernetice. În plus, o astfel de cantitate crescută de date este importantă pentru orice algoritm de învățare automată și inteligență artificială utilizați de intermediari, în vederea antrenării unor astfel de algoritmi pentru a obține un rezultat mai precis.[57]

Ulterior, este esențial să înțelegem limitele legale de partajare pentru a încadra în mod corespunzător obligația legală a intermediarilor și pentru a distinge între răspunderea intermediarilor și răspunderea altor entități/utilizatori. Partajarea datelor analizate include și

---

[50]Araba Vander–Pallen, M., Addai, P., Isteefanos , S., Khan Mohd, T., Survey on Types of Cyber Attacks on Operating System Vulnerabilities din 2018 încoace, 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, SUA, 2022, pp. 01-07, doi : 10.1109/AIIoT54504.2022.9817246.

[51]Pistor, Katharina, Rule by Data: The End of Markets?, 83 Law and Contemporary Problems, pp. 101-124, 2020.

[52]Tremolada, R., Common carriers and public utilities in the digital ecosistem: Unraveling the taxonomy on a quest for better regulation. Legea tehnologiei informației și comunicațiilor, vol. 31(1), pp.35-80, 2022.

[53]Diaconu, DV, Supravegherea video, audio sau fotografierea si patrunderea in spatii private.

[54]Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., van Der Vlist , FN, Weltevrede , E., Studii de aplicații multi-situate: metode și propoziții. Social Media+ Society, vol. 5(2), p.2056305119846486, 2019.

[55]Back, S., LaPrade, J., Prevenirea criminalității cibernetice și amploarea infracțiunilor cibernetice în cadrul instituțiilor de învățământ superior. Jurnalul Internațional de Informații în domeniul securității cibernetice și criminalitate cibernetică, vol. 3(2), pp. 25-47, 2020, https://www.doi.org/10.52306/RGWS2555.

[56]Breen, Casey, Herley, Cormac, Redmiles, Elissa M., A Large-Scale Measurement of Cybercrime Against Individuals, Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22). Association for Computing Machinery, New York, NY, SUA, pp. 1–41, 2022, https://doi.org/10.1145/3491102.3517613.

[57]Moura, José, Serrão , Carlos, Probleme de securitate și confidențialitate ale datelor mari, parte a Manualului de cercetare privind tendințele și direcțiile viitoare în date mari și inteligență web, 2015.

cele către și de la autorități, alți intermediari și alte entități din ecosistemul digital. De asemenea, analizează partajarea datelor brute și a rezultatelor analizelor efectuate de oricare dintre astfel de entități.[58]

Acest capitol se concentrează pe subobiectivul 1.1 și, mai precis, pe ipoteza 1.1.2 și ipoteza 1.1.3. Ipoteza 1.1.2 se referă la limitările care există în ceea ce privește agregarea datelor și ipoteza 1.1.3 privind utilizarea tehnicilor de anonimizare și pseudonimizare pentru analiza datelor agregate. Astfel, capitolul include detalii despre abordarea care trebuie luată pentru a maximiza agregarea și partajarea datelor fără a afecta negativ viața privată a utilizatorilor, valorificând în același timp mecanismele de anonimizare și pseudonimizare care sunt adecvate din perspectiva afacerii și a confidențialității.[59]

Capitolul III.3 vizează elaborarea unor propuneri adecvate pentru asigurarea măsurilor preventive de securitate luate de către intermediari. În acest sens, ține cont de aspectele de intruzivă stabilite în capitolul II cu privire la datele și viața privată a utilizatorilor și a atacatorilor cibernetici și face propuneri de măsuri de securitate tehnice și organizatorice care pot fi luate de intermediari. Capitolul ține cont și de celelalte prevederi legale privind măsurile de securitate preventivă în ecosistemul digital.[60] Accentul este pus pe pașii practici care pot fi întreprinși de intermediari, momentul în care se desfășoară astfel de acțiuni și dacă acestea sunt deja acoperite de legislația existentă sau ar trebui specificate în continuare în legislația specifică. În acest scop, abordarea adoptată este aceea de a avea un răspuns în timp real din partea intermediarilor pe baza informațiilor pe care le dețin la un anumit moment în timp.[61] Acest concept a fost analizat în legislație anterior în contextul aplicațiilor adresate utilizatorilor în Directiva 2 privind serviciile de plăți, Directiva (UE) 2015/2366 privind serviciile de plată pe piața internă și articolul 18 din Regulamentul delegat (UE) 2018/389 al Comisiei. completarea PSD2 din 27 noiembrie 2017, care intră în detaliu și cu anumite aspecte de analizat (model de comportament anormal al utilizatorului, infecție cu malware, locație anormală, locație cu risc ridicat).

Capitolul se concentrează pe subobiectivul 2.1, cu accent pe ipoteza 2.1.1 și 2.1.2, deoarece stabilește situația așa cum este în ceea ce privește obligațiile legale ale intermediarilor, identifică în continuare situațiile în care intermediarii sunt cel mai bine plasați pentru a abordează o anumită problemă de securitate și include propuneri de măsuri preventive pe care intermediarii le pot lua. În acest scop, capitolul analizează tipurile de măsuri tehnice care pot fi luate de intermediari și modul în care acestea pot fi abordate prin legislația existentă, precum și noile cerințe legale propuse.[62]

Titlul IV include analiza limitărilor acțiunilor intermediarilor pentru prevenirea încălcării vieții private a utilizatorilor. În acest scop, analizăm mai întâi cerințele legale propuse pentru intermediari în vederea colectării datelor, analizării datelor și partajării datelor în

---

[58]Garg, Shivi, Baliyan , Niyati, Date privind detectarea vulnerabilităților în Android, Date pe scurt, vol. 22, p. 1081-1087, 2019, https://doi.org/10.1016/j.dib.2018.12.038.

[59]Solove, Daniel J., The Myth of the Privacy Paradox, 89 George Washington Law Review 1, GWU Legal Studies Thesis No. 2020-10, GWU Law School Public Law Thesis No. 2020-10, 2021, https://ssrn.com/abstract=3536265 sau http://dx.doi.org/10.2139/ssrn.3536265

[60]Bank, David, Yamin, Dan, Predicting Cyber-Infections Via Web-Browsing Patterns, 2020, https://ssrn.com/abstract=3757877 sau http://dx.doi.org/10.2139/ssrn.3757877.

[61]Khan, Minhaj Ahmad, Un studiu asupra problemelor de securitate pentru cloud computing, Journal of Network and Computer Applications, voi. 71, p. 11-29, 2016, https://doi.org/10.1016/j.jnca.2016.05.010.

[62]DeNardis, L., Musiani , F., Guvernarea prin infrastructură. În The turn to infrastructure in Internet governance, pp. 3-21, New York: Palgrave Macmillan US, 2016.

vederea asigurării că măsurile de securitate preventivă sunt în vigoare.[63] În al doilea rând, analizăm capacitățile tehnice ale intermediarilor, având în vedere datele la care au acces și controlul/permisiunile pe care le au asupra dispozitivului/conturilor utilizatorului. Limitările tehnice se traduc în limitări legale și limitări ale răspunderii intermediarilor.[64] Având astfel de chestiuni clar stabilite de la început, reduce litigiile pentru clarificări ulterioare. Ulterior, pe baza unor astfel de limitări, acest titlu detaliază modificările propuse la legislația existentă privind protecția datelor și legislația penală în vederea depășirii acestor limitări și a asigurării posibilității măsurilor de securitate asigurate de intermediari și, în același timp, a limitelor tipurilor de măsuri de securitate. care poate fi luat.[65]

Capitolul IV.1 analizează limitările legale din dreptul penal, drepturile omului și protecția datelor cu privire la acțiunile care pot fi întreprinse de intermediari pentru a preveni încălcarea vieții private a utilizatorilor.[66] Aceste limitări apar din cauza necesității accesului la anumite sisteme informatice și la datele utilizatorilor pentru a crea și implementa măsuri de securitate preventivă adecvate. În plus, limitările legale se referă la faptul că anumite acțiuni care pot fi efectuate de intermediari pot avea un impact din perspectiva infracțiunii în viața privată sau asupra sistemelor informatice utilizate de utilizator.[67] Complicațiile suplimentare ale analizei juridice se referă la situația în care dispozitivul utilizat de utilizator este utilizat și de către alte persoane sau în situațiile în care dispozitivul utilizat de utilizator conține date referitoare și la viața privată a altor persoane. În plus, există anumite măsuri legale care pot fi luate de către intermediar pentru a evita răspunderea, având în vedere constrângerile tehnice în luarea de acțiuni după ce efectuează analiza datelor.

Capitolul IV.2 are ca scop construirea pe baza limitărilor legale și recomandările din capitolul IV.1 de mai sus și evidențierea limitărilor tehnice. Aceste limitări pot proveni în primul rând din limitările pure tehnice ale securității în prezent și limitările din partea dispozitivelor din perspectivă tehnică (după cum este detaliat în secțiunea IV.2.1). Limitări specifice pot apărea în ceea ce privește analiza datelor de trafic de la sau către dispozitivul utilizatorului (după cum este detaliat în secțiunea IV.2.5) și vulnerabilități ale altor aplicații sau alți intermediari (după cum este detaliat în secțiunea IV.2.4).[68] O abordare pentru abordarea acestui peisaj larg este stabilirea de standarde și bune practici (după cum este detaliat în secțiunea IV.2.3). Acest lucru oferă claritate cu privire la obligațiile legale ale fiecărei părți interesate și la nivelul controalelor de securitate care trebuie implementate. În al doilea rând, ele pot proveni din limitările tehnice datorate dependențelor de alte entități din ecosistemul

---

[63]Folino, Gianluigi, Sabatino, Pietro, Sisteme de detectare a intruziunilor distribuite și colaborative bazate pe ansamblu: Un sondaj, Journal of Network and Computer Applications, Vol. 66, p. 1-16, 2016, https://doi.org/10.1016/j.jnca.2016.03.011.

[64] Haelterman , Harald, Prevenirea criminalității situaționale și securitatea lanțului de aprovizionare: o considerație „ex ante" a măsurilor preventive, Journal of Applied Security Research 4, nr. 4, p. 483-500, 2009.

[65]Tatar, Unal, Gokce , Yasir, Nussbaum, Brian, Legea versus tehnologie: Blockchain, GDPR și compromisuri dure , Computer Law and Security Review, vol. 38, 2020.

[66]Cath, C., Tehnologia pe care alegem să o creăm: Advocacy pentru drepturile omului în Internet Engineering Task Force. Politica de telecomunicații, 45(6), p.102144, 2021.

[67] Zlati , G., Legitima aparare si starea de necesitate in domeniul criminalitatii informatice , Dreptul , 4/2015, 2015.

[68] Radivilova , T., Kirichenko, L., Ageyev , D., Tawalbeh , M., Bulakh , V., Decriptarea traficului SSL/TLS pentru detectarea amenințărilor ascunse, 2018 a 9-a Conferință internațională IEEE privind sistemele, serviciile și tehnologiile de încredere (DESERT) , p. 143-146, 2018, doi : 10.1109/DESERT.2018.8409116.

digital[69] (după cum este detaliat în secțiunea IV.2.2). În al treilea rând, trebuie avut în vedere și aspectul performanței, deoarece instrumentele de securitate pot avea un impact mare asupra performanței hardware-ului și software-ului din dispozitivul utilizatorului (așa cum este detaliat în secțiunea IV.2.6).[70]

Acest capitol este legat de două subobiective. Acesta detaliază anumite puncte referitoare la subobiectivul 2.1 în legătură cu ipoteza 2.1.3 privind cooperarea fiind o cerință pentru asigurarea unei preveniri adecvate. În ceea ce privește subobiectivul 2.2, capitolul abordează ipoteza 2.2.3 în sensul că include anumite limitări tehnice care trebuie avute în vedere atunci când se evaluează obligația intermediarilor de a preveni încălcările vieții private și ipoteza 2.2.4. în ceea ce privește limitările de performanță care reduc și tipurile de măsuri de securitate care pot fi luate pe un anumit dispozitiv.[71] În esență, toate aceste limitări tehnice sau organizatorice au un impact asupra numărului de încălcări reușite ale vieții private a utilizatorilor și ar trebui identificate în mod clar pentru a preveni răspunderea civilă, administrativă sau penală a intermediarilor pentru neprevenirea acestora, după cum se detaliază mai jos.

Cercetarea include analiza legislației la nivelul UE și a legislației românești privind dreptul penal, protecția datelor și drepturile omului. Alte unghiuri sunt, de asemenea, relevante, de exemplu, dreptul concurenței și protecția consumatorilor. Cu toate acestea, acestea nu sunt în centrul acestei cercetări. În plus, cercetarea se concentrează asupra celor două obiective de mai sus în ceea ce privește identificarea rolului intermediarilor în prevenirea potențialelor infracțiuni, fără a participa la acțiunile penale în sine. [72]Din această cercetare rezultă un set de prevederi legale propuse în acest sens. Astfel de propuneri sunt validate și printr-o abordare cantitativă. Cu toate acestea, poate fi efectuată o validare suplimentară a evaluării impactului unor astfel de propuneri, inclusiv impactul acestora din alte perspective decât dreptul penal, protecția datelor și dreptul drepturilor omului.[73]

Subliniem mai jos câteva unghiuri ale conceptului de viață privată neincluse în această teză și care pot constitui subiecte de cercetare viitoare în acest domeniu:

- Analiza datelor (în special în contextul big data), împreună cu orice activități de profilare sau urmărire și orice decizii automate referitoare la persoane (care pot crea consecințe juridice sau efecte similare asupra persoanelor).[74]

---

[69]Karagiannis, C. Dovezi digitale „ascunse în nor": „posesiunea" este încă o noțiune relevantă?. ERA Forum 23, pp. 301–311, 2023. https://doi.org/10.1007/s12027-022-00724-7

[70]Madala, Ravikiran, A Novel Dynamic Watermarking for Secure Data Protection from Cyber Theft Based on Artificial Intelligence Supervision, 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), 2023, https://ssrn.com/abstract=4475548.

[71]Zhou, Chenfeng Vincent, Leckie, Christopher, Karunasekera , Shanika, Un studiu asupra atacurilor coordonate și a detectării intruziunilor în colaborare, Computers and Security, vol. 29, Numărul 1, p. 124-140, 2010, https://doi.org/10.1016/j.cose.2009.06.008.

[72] Slavoiu , Radu, Protectia penala a vietii private, Universul Juridic, pag . 138, 2016.

[73]Bianchi, G. et al., Towards Privacy-Preserving Network Monitoring: Issues and Challenges, 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Atena, Grecia, pp. 1-5, 2007, doi : 10.1109/PIMRC .2007.4394186.

[74]AEPD, Conducerea prin exemplu: Strategia AEPD 2015-2019, pag . 17. „Datele mari", în opinia noastră, „se referă la practica de a combina volume uriașe de informații provenite din diverse surse și de a le analiza, folosind adesea algoritmi de auto-învățare pentru a informa deciziile. Una dintre cele mai mari valori ale datelor mari pentru întreprinderi și guverne este derivată din monitorizarea comportamentului uman, colectiv și individual, și rezidă în potențialul său predictiv; Avizul AEPD 4/2015, Către o nouă etică digitală: date, demnitate și tehnologie,

- Protecția consumatorilor (inclusiv cerințele specifice referitoare la copii) [75]și implicațiile legislației concurenței în cazul schimbului de date.[76]
- Specificații privind partajarea datelor în cazul unei relații între angajator și angajat, inclusiv aspecte legate de monitorizarea activității online a angajaților.
- Remedii pentru prejudiciile aduse de încălcarea confidențialității, inclusiv daunele plătite persoanelor fizice sau altor companii pe baza răspunderii delictuale sau contractuale (inclusiv cererile de asigurare cibernetică). CEDO [77]a definit în linii mari conceptul de viață privată (care are unele legături cu conceptele de confidențialitate și date cu caracter personal), inclusiv orice informații despre viața privată și de familie, reședință, corespondență (e-mail, telefon, e-mail la locul de muncă).[78]

În plus, obligațiile legale de prevenire ar trebui să includă atât considerente de drept penal, cât și de drept civil. În plus, acestea ar trebui să reflecte și ar trebui interpretate de către instanțele de judecată în lumina limitărilor tehnice și a capacităților tehnice legate de astfel de situații. În acest deceniu, legislația s-a dezvoltat pentru a ajunge din urmă cu peisajul tehnologic în continuă schimbare.

Legislația sa concentrat în mod semnificativ pe organizarea internă a entităților în vederea implementării bunelor practici de securitate adecvate și, de asemenea, pe ciclul de viață securizat al dezvoltării software. Din acest motiv, am ales să ne concentrăm asupra unui decalaj existent în legislația existentă, respectiv, rolul intermediarilor în asigurarea măsurilor de securitate preventivă în vederea protejării vieții private a persoanelor care utilizează serviciile intermediarului.

Pentru a arăta utilitatea de a avea obligații legale pentru intermediari în cadrul unei anumite activități, ne-am uitat la legislația împotriva spălării banilor care a impus de-a lungul anilor din ce în ce mai multe obligații intermediarilor operațiunilor de spălare a banilor, inclusiv bănci etc. Astfel, în vederea depistarii unor astfel de infracțiuni și, ulterior, în vederea asigurării unor măsuri preventive împotriva acestora, legiuitorul a optat pentru a avea obligații bazate pe intermediarii implicați în ecosistem.[79]

2015. AEPD, Avizul 7/2015 Întâmpinarea provocărilor date mari, 2015. AEPD, Avizul 8/2016 Aviz privind aplicarea coerentă a drepturilor fundamentale în epoca big data, 2016.

[75]Comisia pentru energie și comerț a Camerei Reprezentanților SUA, audiere intitulată „Algoritmi: cum deciziile companiilor despre date și conținut impactează consumatorii" 2017, http://docs.house.gov/meetings/IF/IF17/20171129/106659/HHRG- 115-IF17-20171129-SD002.pdf , ultima accesare la 24 decembrie 2022. Departamentul de Comerț, Grupul operativ pentru politicile de internet, securitatea cibernetică, inovația și economia internetului, 2011.

[76]Goldfarb, Avi și Tucker, Catherine, Confidențialitate și inovație, 12 INNOVATION POL'Y și ECON. 65, 2012.

[77]CEDO, Klass și alții împotriva Germaniei, cauza nr. 5029/71, alin. 55-60, Cauza Von Hannover împotriva Germaniei nr. 40660/08 și 60641/08, alin. 50-53, Sciacca împotriva Italiei, cauza nr. 50774/99, alin. 27-30, dosarul Rotaru împotriva României nr. 28341/95, alin. 59-60; PG și JH împotriva cauzei Regatul Unit nr. 44787/98, alin. 61-63; Peck împotriva Regatului Unit nr. 44647/98, alin. 102-104; Cauza Amann împotriva Elveției nr. 27798/95, alin. 75-80.

[78]Duca, Maria Violeta, Răspunderea patrimonială A angajatorului . Supravegherea nelegală a modalității de utilizare a laptopului si telefonului de serviciu . Daune moral pentru intruziunea în viata privată a salariaților , Revista Romană de Jurisprudenta 2/2018, 2018. Curtea de Apel București, decizia nr. 3033/2018.

[79]Recomandarea CM/ Rec(2018)2 a Comitetului de Miniștri către statele membre privind rolurile și responsabilitățile intermediarilor internet adoptată de Consiliul Europei în aprilie 2018.