CZU: 343.221:004.738.5 **http://doi.org/10.59295/sum8(168)2023_26**

ANONIMITATEA PE INTERNET *VERSUS* INDENTIFICAREA INFRACTORILOR

Gheorghe RENIȚĂ,
Universitatea de Stat din Moldova

Tot mai multe persoane aleg să acționeze pe Internet în anonimat. Acest fapt generează multe beneficii, în special, încurajează exprimarea opiniilor critice. Pe de altă parte, există și o „parte întunecată” a acestui fenomen. Mai exact, făptuitorii pot opta pentru comiterea infracţiunilor pe Internet în anonimat. În acest articol se susține că anonimitatea pe Internet nu trebuie să constituie un obstacol pentru aflarea adevărului și, respectiv, pentru înfăptuirea justiției. Așadar, confidențialitatea pe Internet trebuie să cedeze atunci când în joc se află imperativul identificării infractorilor și al despăgubirilor victimelor. Totuși, acest lucru trebuie să se facă cu respectarea unor garanții, nu în mod arbitrar.

Cuvinte-cheie: *anonimitate, Internet, conturi false pe rețele de socializare, dreptul la viață privată, obligație pozitivă, anchetă efectivă, infractor.*

ANONYMITY ON THE INTERNET *VERSUS* IDENTIFICATION OF OFFENDERS

More and more people choose to act anonymously on the Internet. This fact generates many benefits, for example, it encourages the expression of critical opinions. On the other hand, there is also a "dark side" to this phenomenon. Specifically, perpetrators can opt to commit crimes on the Internet anonymously. This article argues that anonymity on the Internet should not be an obstacle to finding out the truth and, respectively, to the administration of justice. So, Internet privacy must yield when the imperative of identifying offenders and reparations to victims is at stake. However, this must be done with safeguards in mind, not arbitrarily.

Keywords: *anonymity, Internet, fake accounts on social networks, right to privacy, positive obligation, effective investigation, offender.*

Introducere

Internetul și tehnologiile informaționale au generat o serie de beneficii, inclusiv pentru exercitarea unor drepturi fundamentale (*e.g.*, dreptul la educație, dreptul la libera exprimare).

În acelaşi timp, Internetul și tehnologiile informaționale pot reprezenta „instrumente” utile pentru comiterea unor infracțiuni și, respectiv, pentru încălcarea unor drepturi fundamentale (*e.g.*, dreptul la viață privată).

Persoanele pot opta, din varii motive, să acționeze pe Internet în anonimat, cu un nume fals, cu un pseudonim etc. Unul dintre aceste motive ar putea constitui dorința persoanei de a nu fi identificată, mai ales atunci când aceasta a comis o faptă incriminată de legea penală (*e.g.*, determinarea la sinucidere).

Anonimitatea pe Internet [1] poate constitui, uneori, un obstacol [2] pentru identificarea persoanelor care au comis fapte penale în vederea tragerii lor la răspundere și, în consecință, a înfăptuirii justiției. Acest aspect a fost accentuat și în literatura de specialitate [3].

În acest studiu voi analiza în ce măsură anonimitatea pe Internet se conciliază cu obiectivul de identificare a persoanelor care au comis infracțiuni prin intermediul tehnologiilor informaționale. Pentru atingerea acestui scop voi face apel la prevederile normative relevante, precum și la jurisprudența Curții Europene a Drepturilor Omului (în continuare – Curtea Europeană).

Rezultate și discuții

Cu titlu preliminar, încă în 1995, Comitetul de Miniștri al Consiliului Europei a adoptat Recomandarea nr. R(95)13 privind problemele de procedură penală legate de tehnologiile informaționale, conform căreia [4]:

„9. Sub rezerva privilegiilor sau protecției, majoritatea sistemelor juridice (...) ar trebui să se prevadă prerogativele de a ordona unor persoane să prezinte orice date specifice aflate în controlul lor într-un sistem informatic, în forma cerută de către autoritatea de investigare.

10. Sub rezerva privilegiilor sau protecției, autoritățile de investigație trebuie să aibă prerogativa să ordoneze persoanelor care au în controlul lor date într-un sistem informatic, să furnizeze toată informația necesară pentru a permite accesul la sistemul informatic și la datele aferente acestuia. Legea procesual penală trebuie să se asigure că un ordin similar poate fi dat altor persoane care cunosc despre funcționarea unui sistem informatic sau despre măsurile aplicate pentru securizarea datelor aferente acestuia.

(...)

12. Prestatorilor de servicii care oferă servicii de telecomunicații publicului trebuie să le fie impuse obligații specifice, prin intermediul rețelelor publice ori private, să ofere informații pentru identificarea utilizatorului, la ordinul autorității competente de investigare."

Aceste deziderate au fost materializate în Convenția Consiliului Europei privind criminalitatea informatică (Budapesta, 23 noiembrie 2001) [5], Convenție pe care Republica Moldova a ratificat-o în 2009 [6]. Conform art. 18 (intitulat „Ordinul de punere la dispoziţie a datelor") din această Convenție:

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a conferi autorităţilor sale competente dreptul de a ordona:

a) unei persoane prezente pe teritoriul său să comunice datele informatice menţionate, aflate în posesia sau sub controlul său, care sunt stocate într-un sistem informatic ori pe un suport de stocare informatic; şi

b) unui furnizor de servicii care oferă prestaţii pe teritoriul părţii să comunice datele din posesia sau de sub controlul său referitoare la abonaţi şi la astfel de servicii.

(...)

3. În sensul prezentului articol, expresia date referitoare la abonaţi va desemna orice informaţie, sub formă de date informatice sau sub orice altă formă, deţinută de un furnizor de servicii, referitoare la abonaţii acestor servicii, altele decât datele referitoare la trafic sau conţinut, şi care permit stabilirea:

a) tipului de serviciu de comunicaţii utilizat, dispoziţiilor tehnice luate în această privinţă şi perioadei serviciului;

b) identităţii, adresei poştale sau geografice, numărului de telefon al abonatului şi oricărui alt număr de contact, precum şi a datelor referitoare la facturare şi plată, disponibile în baza unui contract sau a unui aranjament de servicii;

c) oricărei alte informaţii referitoare la locul în care se găsesc echipamentele de comunicaţie, disponibile în baza unui contract sau a unui aranjament de servicii."

Mai mult, cel de al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică [7] referitor la cooperarea consolidată și la divulgarea probelor electronice [8] prevede la art. 7 § 1 următoarele:

„Fiecare parte (*i.e.* – stat membru la Convenție) adoptă măsurile legislative și de altă natură necesare pentru a împuternici autoritățile sale competente să emită un ordin care să fie transmis direct unui furnizor de servicii de pe teritoriul altei părți, pentru a obține dezvăluirea abonatului specificat, stocat, informații aflate în posesia sau controlul respectivului furnizor de servicii, în cazul în care informațiile abonatului sunt necesare pentru anchetele sau procedurile penale specifice ale părții emitente."

Așadar, există un consens european care instituie în sarcina prestatorilor de servicii de Internet obligația de a comunica date care ar permite identificarea infractorului.

La nivel național, conform art. 5 din Legea nr. 20 din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice [9], în cadrul activităţilor de prevenire şi combatere a criminalităţii informatice, autorităţile competente, furnizorii de servicii[1], organizaţiile neguvernamentale, alţi reprezentanţi ai societăţii civile colaborează prin schimb de informaţii, de experţi, prin activităţi comune de cercetare a cazurilor şi de identificare a infractorilor (sublinierea îmi aparține – n.a.), de instruire a personalului, prin realizarea de iniţiative în scopul promovării unor programe, practici, măsuri, proceduri şi standarde minime de securitate

[1] Potrivit art. 2 din Legea nr. 20 din 3 februarie 2009 privind prevenirea și combaterea criminalității informatice, prin „furnizor de servicii" se are în vedere orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic, precum și orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicații sau pentru utilizatorii săi.

a sistemelor informatice, prin campanii de informare privind criminalitatea informatică şi riscurile la care sunt expuşi utilizatorii de sisteme informatice, prin alte activităţi în domeniu.

Iar în baza art. 7 alin. (1) din aceeași lege, furnizorii de servicii sunt obligaţi:

a) să ţină evidenţa utilizatorilor de servicii;

b) să comunice autorităţilor competente datele despre traficul informatic, inclusiv datele despre accesul ilegal la informaţia din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, la denaturarea sau la distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte delicte informatice;

c) să execute, în condiţii de confidenţialitate, solicitarea autorităţii competente privind conservarea imediată a datelor informatice ori a datelor referitoare la traficul informatic, faţă de care există pericolul distrugerii ori alterării, pe un termen de până la 120 de zile calendaristice, în condiţiile legislaţiei naţionale;

d) să prezinte autorităţilor competente, în temeiul unei solicitări efectuate în condiţiile legii, date referitoare la utilizatori, inclusiv la tipul de comunicaţie şi la serviciul de care a beneficiat utilizatorul, la modalitatea de plată a serviciului;

e) să întreprindă măsuri de securitate prin utilizarea unor proceduri, dispozitive sau programe informatice specializate cu al căror ajutor accesul la un sistem informatic să fie restricţionat sau interzis utilizatorilor neautorizaţi;

e[1]) să sisteze, în condițiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce contribuie la comiterea infracțiunilor sau la încălcarea prevederilor legislației în vigoare ori conțin/difuzează instrucțiuni privind modul de comitere a acestora;

f) să asigure monitorizarea, supravegherea şi păstrarea datelor referitoare la trafic, pe o perioadă de 180 de zile calendaristice, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii şi a canalului prin al cărui intermediu comunicația a fost transmisă;

g) să asigure descifrarea datelor informatice care se conţin în pachetele protocoalelor de reţea cu conservarea acestor date pe o perioadă de 90 de zile calendaristice.

Deși unele dintre prevederile citate mai sus pot genera probleme de interpretare și, respectiv, de aplicare (*e.g.*, nu este clar care sunt acele „condiții prevăzute de lege” care permit sistarea accesului din propriul sistem informatic la toate adresele IP pe care sunt amplasate pagini web), trebuie de remarcat că, *de lege lata*, există o obligație specifică din partea furnizorilor de servicii de telecomunicații să prezinte date informatice, inclusiv date despre abonați, ca răspuns la o cerere formulată de organul de urmărire penală sau de instanța de judecată [10].

Rațiunea acestei obligații rezidă în necesitatea efectuării unei investigații/anchete efective. În accepția Curții Europene a Drepturilor Omului, pentru ca o anchetă să fie considerată „efectivă”, aceasta trebuie, în principiu, să fie de natură să conducă la stabilirea circumstanțelor cauzei și la identificarea și pedepsirea celor responsabili [11, 12]. Efectuarea unei investigații efective reprezintă o obligație pozitivă (procedurală) de mijloace, nu de rezultat. Această obligație poate să derive, spre exemplu, din art. 2 (dreptul la viață), din art. 3 (interzicerea torturii) sau din art. 8 (dreptul la respectarea vieții private și de familie) din Convenția Europeană a Drepturilor Omului (în continuare – Convenția).

Totodată, persoanele vizate ar putea pretinde că prin furnizarea unor informații despre ei (în particular, a unor date care permit identificare persoanei – numele și prenumele, anul și data nașterii, codul personal etc.), s-ar încălca dreptul la protecția datelor cu caracter personal sau, mai generic spus, dreptul la viață privată. Acest drept este garantat, între altele, de art. 28 din Constituție și de art. 8 din Convenția Europeană a Drepturilor Omului. Dar acest drept nu este absolut. El poate fi restrâns.

În căutarea unui echilibru corect [13] între, pe de o parte, protecția dreptului la viață privată și, pe de altă parte, imperativul identificării presupusului infractor care a acționat pe Internet sub anonimat voi face apel la jurisprudența Curții Europene.

Voi debuta cu speța *K.U. v. Finlanda* în care Curtea Europeană a evidențiat principiile generale privind obligația pozitivă a autorităților de a asigura respectarea dreptului la viața privată în sfera relațiilor dintre privaţi. Circumstanţele cazului pot fi rezumate după cum urmează. O persoană necunoscută a publicat un anunț de natură sexuală pe un sit Internet de întâlniri, în numele reclamantului, care avea doisprezece ani la acel moment, fără cunoștința acestuia. Anunțul oferea detalii privind vârsta reclamantului, anul nașterii și trăsăturile fizice, spunând că acesta era în căutarea unei relații intime cu un bărbat. Anunțul conținea, de asemenea, un link cu trimitere la pagina web a reclamantului, unde puteau fi găsite fotografia și numărul lui de telefon. Reclamantul a aflat de anunț atunci când a primit un e-mail de la un bărbat care îi propunea să se întâlnească și „apoi să vadă ce dorește".

Tatăl reclamantului a cerut poliției să identifice persoana care a plasat anunțul pentru a înainta pretenții împotriva acesteia, însă furnizorul de servicii Internet a refuzat să divulge identitatea titularului adresei IP în cauză, considerându-se obligat să păstreze confidențialitatea datelor abonaților. Poliția a cerut instanței de judecată să oblige furnizorul de servicii să divulge informația respectivă, bazându-se pe prevederi normative ce reglementau urmărirea penală. Instanța a respins această solicitare, subliniind că nu exista nicio prevedere legală expresă pentru a obliga un furnizor de servicii internet să nu țină cont de regulile referitoare la secretul profesional și să divulge informația cerută în cauzele ce vizau infracțiuni mai puțin grave, cum ar fi calomnia. Curtea de Apel a confirmat această decizie, iar Curtea Supremă a declarat recursul inadmisibil.

Pe scurt, identitatea persoanei care a plasat anunțul nu a putut fi, totuși, obținută de la furnizorul de Internet din cauza legislației în vigoare la acel moment în Finlanda [14].

În fața Curții Europene, reclamantul a pretins, în special, că statul nu și-a onorat obligațiile sale pozitive de a-i proteja dreptul la respectarea vieții private în baza articolului 8 al Convenției.

Potrivit Curții Europene, în lipsa mijloacelor de a identifica infractorul real și de a-l aduce în fața justiției, existența unei infracțiuni are efecte de descurajare limitate. Aici, Curtea a notat că nu este exclusă posibilitatea ca obligațiile pozitive ale statului în baza art. 8 din Convenție de a proteja integritatea fizică sau psihică a persoanelor pot fi extinse la chestiunea privind eficiența unei anchete penale, chiar dacă nu este vorba despre răspunderea penală a agenților statului. Pentru Curte, statele au o obligație pozitivă inerentă în art. 8 al Convenției de a incrimina infracțiunile împotriva persoanei, inclusiv tentativele de infracțiune, și de a consolida efectul descurajator al incriminării prin aplicarea prevederilor de drept penal în practică, prin intermediul unei urmăriri penale eficiente. În cazul în care este amenințată integritatea fizică și psihică a unui copil, interdicția dobândește o importanță și mai mare. Curtea a reamintit, în acest sens, că abuzul sexual este, fără îndoială, un delict odios, cu efecte debilitante asupra victimelor sale. Copiii și alte persoane vulnerabile au dreptul la protecție din partea statului, în forma unei descurajări eficiente, de la aceste forme grave de ingerință în aspectele esențiale ale vieților lor private [15].

Curtea Europeană a repudiat argumentul Guvernului Finlandei, precum că reclamantul a avut posibilitatea de a obține prejudicii de la un terț, și anume de la furnizorul de servicii. Curtea a considerat că acesta nu a fost suficient în circumstanțele acestei cauze. Este clar că atât interesul public, cât și protecția intereselor victimelor infracțiunilor comise împotriva integrității lor fizice și psihice necesită existența unui remediu care permite ca infractorul real să fie identificat și adus în fața justiției, în această cauză, acesta fiind persoana care a plasat anunțul în numele reclamantului, și ca victima să obțină reparație materială din partea acestuia [16].

Curtea Europeană a acceptat că, având în vedere dificultățile existente în reglementarea societăților moderne, obligația pozitivă trebuie să fie interpretată într-un mod care nu impune o sarcină imposibilă sau disproporționată pentru autorități sau, în acest caz, pentru legislator. Un alt argument relevant este nevoia de a asigura ca prerogativele de control, prevenire și investigare a infracțiunilor să fie exercitate într-un mod care respectă pe deplin un proces echitabil și alte garanții care impun restricții, în mod legitim, privind investigarea infracțiunilor și aducerea infractorilor în fața justiției, inclusiv garanțiile conținute în articolele 8 (dreptul la respectarea vieții private și de familie) și 10 (libertatea de exprimare) din Convenție, garanții pe care însăși infractorii se pot baza. Curtea este sensibilă la argumentul Guvernului precum că orice deficiență legislativă urmează a fi privită în contextul social la momentul producerii faptelor. Curtea a notat, în același timp, că incidentul în cauză a avut loc într-un moment când era bine-cunoscut faptul că Internetul, tocmai

din cauza caracterului său anonim, putea fi folosit în scopuri criminale. De asemenea, problema răspândită a abuzului sexual al copiilor a devenit bine-cunoscută în ultima perioadă. Prin urmare, nu se poate spune că Guvernul pârât nu a avut posibilitatea de a implementa un sistem de protecție a copiilor victime – ținte ale avansurilor din partea pedofililor, prin intermediul Internetului [17].

Așadar, Curtea Europeană a considerat că protecția practică și eficientă a reclamantului a necesitat luarea de măsuri eficiente pentru a identifica și a urmări în justiţie infractorul, adică persoana care a plasat anunțul. În această cauză, o asemenea protecție nu a fost oferită. O urmărire penală eficientă nu a putut fi avansată din cauza exigențelor de confidențialitate. Deși libertatea de exprimare și confidențialitatea comunicațiilor sunt preocupări primordiale și utilizatorii telecomunicațiilor și a Internetului trebuie să aibă garanția că viața lor privată și libertatea de exprimare vor fi respectate, o asemenea garanție nu poate fi absolută și trebuie să cedeze uneori altor imperative legitime, cum ar fi prevenirea dezordinii sau infracțiunilor ori protecția drepturilor și libertăților altuia. Fără a analiza aspectul dacă comportamentul persoanei care a plasat anunțul criminal pe Internet putea atrage protecția articolelor 8 și 10 din Convenție, având în vedere natura sa condamnabilă, în opinia Curții a fost, totuși, sarcina legislatorului de a oferi cadrul necesar pentru reconcilierea diferitor interese care concurează pentru protecție în acest context. Totuși, un astfel de cadru nu a fost în vigoare la momentul desfășurării evenimentelor, astfel încât Finlanda nu poate fi eliberată de obligația sa pozitivă în privința reclamantului [18].

Din aceste motive, Curtea Europeană a constatat că a existat o încălcare a dreptului la viață privată a reclamantului și i-a acordat 3000 de euro cu titlu de prejudiciu moral.

Având în vedere circumstanţele particulare ale cazului *K.U. v. Finlanda*, făptuitorul nu ar fi putut să pretindă, în mod plauzibil, că prin anunțul postat și-ar fi exercitat dreptul la libera exprimare. Dreptul la libera exprimare trebuie exercitat în interiorul anumitor limite [19], limite care, cu certitudine, nu acoperă situația din speță. În schimb, în acest caz a existat un conflict între principii în interiorul dreptului la viață privată (*i.e.*, un conflict între diferite aspecte ale dreptului la viață privată). Pe de o parte, principiul aflării adevărului care dă în vileag interesul victimei de identificare a făptuitorului pentru a putea cere urmărirea acestuia în justiție și, respectiv, repararea prejudiciului pentru încălcarea dreptului la viață privată. Pe de altă parte, principiul confidențialității datelor personale ale făptuitorului care a acționat pe Internet în anonimat. Ambele principii sunt importante.

Din punct de vedere conceptual, „principiile constituie norme care cer realizarea unui lucru în cea mai mare măsură posibilă, date fiind posibilitățile factuale și juridice. Așadar, principiile sunt cerințe de optimizare. Ca atare, ele sunt caracterizate de faptul că pot fi realizate în grade diferite. Mai mult, gradul adecvat al realizării lor nu depinde doar de ceea ce este posibil din punct de vedere factual, ci și de ceea ce este posibil din punct de vedere juridic” [20].

Stabilirea gradului adecvat de realizare a unui principiu relativ, față de cerințele celorlalte principii are loc prin intermediul punerii în balanță [21]. Astfel, punerea în balanță reprezintă forma specială a aplicării principiilor [22].

Așadar, conflictul dintre principii poate fi rezolvat prin punerea în balanță. După Robert Alexy, esența punerii în balanță constă într-o relație care poate fi denumită „Legea Punerii în Balanță” și care poate fi formulată după cum urmează:

„Cu cât mai mare este gradul nerealizării sau al prejudicierii unui principiu, cu atât mai mare trebuie să fie importanța realizării celuilalt” [23].

Natura principiilor ca cerințe de optimizare presupune existența unei legături necesare între principii și analiza proporționalității [24].

Totodată, în contextul stabilirii echilibrului corect între principii, Aharon Barak pledează pentru compararea (i) importanței sociale a evitării lezării dreptului persoanei cu (ii) importanța socială a beneficiului câștigat prin îndeplinirea scopului legitim urmărit de către stat [25].

În cazul *K.U. v. Finlanda* legislatorul a eșuat să stabilească, la modul abstract, un echilibru corect între principiile concurente. El a conferit confidențialității datelor persoanelor care acționează pe Internet sub anonimat o pondere mare în detrimentul imperativului identificării persoanelor care încalcă drepturi fundamentale, în speță, dreptul la viață privată. Acest fapt a condus la condamnarea statului pentru încălcarea

art. 8 din Convenția Europeană a Drepturilor Omului, pentru că nu și-a îndeplinit obligațiile pozitive care derivă din acest articol în raport cu victimele cărora li s-au lezat dreptul la viață privată.

Un alt caz relevant îl constituie *Volodina v. Rusia (nr. 2)*, în care Curtea Europeană a constatat, între altele, că autoritățile nu au trimis nicio solicitare către o rețea de socializare vizată (în speță, era vorba de Instagram) pentru a identifica proprietarul conturilor false, conturi pe care erau plasate pozele intime ale reclamantei [26]. Deși poliția a inițiat o anchetă penală în baza art. 137 din Codul penal al Federației Ruse („Încălcarea inviolabilităţii vieţii personale"), procesul penal a fost încetat, pentru că a expirat termenul de prescripție [27]. Din nou, Curtea Europeană a constatat că statul nu a întreprins o anchetă efectivă și că a încălcat, între altele, art. 8 din Convenția Europeană a Drepturilor Omului.

Și Republica Moldova a fost condamnată de către Curtea Europeană pentru eșecul autorităților naționale de a-și îndeplini obligațiile pozitive, prin desfășurarea unei anchete efective, pentru asigurarea protecției adecvate împotriva ingerințelor grave în viața privată a persoanei. Am în vedere cazul *Straistă v. Republica Moldova*.

În acest caz, Curtea Europeană a stabilit că, în 2012, a fost creat un profil fals pe Facebook, fiind utilizate numele și fotografiile reale ale reclamantei, precum și alte fotografii care înfățișau o femeie îmbrăcată sumar în ipostaze provocatoare, cu fața ascunsă. Textul sub fotografii relata despre faptul că aceasta presta servicii sexuale. Era indicat și numărul de telefon real al reclamantei. Per total, în perioada 2012-2013, peste 50 de conturi de acest gen au fost create pe Facebook, în timp ce conturi similare au fost create și pe alte rețele de socializare. Numeroasele plângeri ale reclamantei către autorități au constituit temei pentru intentarea unor proceduri contravenţionale, care au fost încetate în martie 2014, din cauza expirării termenului de prescripție; reclamanta fiind informată despre aceasta abia în ianuarie 2015. Adresa IP de la care au fost create conturile (obținută de către reclamantă de la Facebook) nu ar fi fost verificată de către autorități. Profiluri similare au continuat să fie create pe Facebook până în anul 2015; de fiecare dată reclamanta s-a plâns autorităților [28].

Curtea Europeană a reiterat că în martie 2014, ancheta a fost încetată din cauza expirării termenului de prescripție. Totuși, reclamanta s-a plâns, de mai multe ori, cu privire la noile conturi denigratoare create utilizând numele său, inclusiv după martie 2014. Prin urmare, expirarea termenului de prescripție nu putea fi un motiv întemeiat pentru încetarea anchetei, deoarece noile atacuri comise, în mod regulat, la adresa vieții private a reclamantei erau identice cu cele anterioare și, astfel, erau parte dintr-o încălcare continuă a drepturilor sale. Mai mult, Guvernul nu a prezentat nicio dovadă a vreunei măsuri concrete întreprinse, în special a solicitării de la operatorii autohtoni de acces la internet a identității persoanei care utiliza adresa IP transmisă de către reclamantă. De asemenea, aceasta nu a fost informată, fiind nevoită să depună plângeri pentru a afla despre deciziile luate pe caz. În consecință, Curtea a conchis, în unanimitate, că a existat o încălcare a art. 8 din Convenție și i-a acordat reclamantei 5000 de euro cu titlu de prejudiciu moral [29].

Spre deosebire de cazul *K.U. v. Finlanda* – în care problema centrală a fost plasată pe umerii legislatorului, - în *Volodina v. Rusia (nr. 2)* și în *Straistă v. Republica Moldova* legislația națională permitea obținerea datelor susceptibile să conducă la identificarea făptuitorului, însă autoritățile nu au făcut acest lucru. Inacțiunea autorităților, în special, a organului de urmărire penală, a condus la încălcarea Convenției.

Totodată, nu este clar: prin prisma cărei norme din Codul contravențional au fost privite, de către poliție, faptele din cazul *Straistă v. Republica Moldova*. Acest aspect nu a fost redat în hotărârea Curții Europene. Probabil, poliția ar fi apreciat că faptele în discuție constituie o calomnie. Într-o cauză judecată de Judecătoria Chișinău s-au atestat fapte oarecum similare cu cele din cazul *Straistă v. Republica Moldova*, însă s-a aplicat Codul penal, nu Codul contravențional. Mai exact, Judecătoria Chișinău a constatat că *în perioada 28 februarie 2017 – 14 martie 2017, fără a avea consimțământul lui I. C., dispunând de poze ale acesteia în ipostaze intime, pe care le-a făcut în perioada concubinajului, recurgând la falsul de identitate, B. V. a creat pe site-ul www.instagram.com o pagină web cu denumirea „y.c.". B. V. a postat pe această pagină unsprezece poze în care I. C. apărea nudă. Motivul acestei acțiuni l-a constituit faptul că I. C. nu a dorit să continue relațiile cu B. V. Ulterior, B. V. a redenumit pagina web respectivă în „sterva_y" şi a postat alte treizeci și una de fotografii în care I.C. apărea nudă și/sau angajată în raporturi sexuale. Pozele în cauză au devenit accesibile unui cerc nedeterminat de persoane. Ulterior, B. V. a expediat pozele respective lui D. I., mătușa lui I. C., precum și lui L. C., sora lui I. C.* [30].

Pentru aceste fapte, instanţa de judecată a considerat incident art. 177 alin. (1) („Încălcarea inviolabilităţii vieţii personale”) din Codul penal (articol care stabilește răspunderea pentru culegerea ilegală sau răspândirea cu bună-ştiinţă a informaţiilor, ocrotite de lege, despre viaţa personală ce constituie secret personal sau familial al altei persoane fără consimțământul ei) și i-a aplicat lui B.V. pedeapsa amenzii în mărime de 500 de unități convenționale, ceea ce constituie 25000 de lei.

În literatura de specialitate s-a arătat, just, că „întru asigurarea plenitudinii calificării, în astfel de cazuri, alături de art. 177 din Codul penal, urmează a fi aplicat art. 90 din Codul contravențional, care stabileşte răspunderea pentru producerea, comercializarea, difuzarea sau păstrarea produselor pornografice pentru a fi comercializate ori difuzate. Această faptă contravențională rezidă în pornografia adultă, având, sub aspectul vârstei victimei, rolul de antiteză în raport cu infracțiunea prevăzută la art. 208[1] din Codul penal” [31].

Potrivit acelorași autori, „dacă imaginile sau alte reprezentări pornografice distribuite sunt însoțite de informaţii mincinoase ce defăimează cu bună-știință victima (de exemplu, de informații în formă scrisă că victima prestează servicii sexuale în schimbul unei remunerații), devine aplicabil, de asemenea, art. 70 alin. (1) din Codul contravențional, care prevede răspunderea pentru calomnie” [32].

Prin urmare, faptele din cazul *Straistă v. Republica Moldova* nu trebuiau privite doar din perspectiva calomniei, ci și a art. 177 alin. (1) din Codul penal și, eventual, a art. 90 din Codul contravențional (asta sub rezerva în care fotografiile cu pretinsa „îmbrăcăminte sumară” și cu pretinsele „ipostaze provocatoare” ar fi fost considerate pornografice[2]).

În contrast, mai trebuie de remarcat că în practica judiciară a României s-a decis că „fapta de a deschide şi utiliza un cont pe o reţea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane şi introducând date personale reale care permit identificarea acesteia, întruneşte două dintre cerinţele esenţiale ale infracţiunii de fals informatic prevăzute în art. 325 din Codul penal [al României][3], respectiv cea ca acţiunea de introducere a datelor informatice să fie realizată fără drept şi cea ca acţiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului” [33]. Aceste explicații pot fi extrapolate și în raport cu art. 260[5] („Falsul informatic”) din Codul penal al Republicii Moldova[4], care are un conținut aproape identic cu cel de la art. 325 din Codul penal al României.

Trecând de la general spre particular, într-o speță din practica judiciară a României, s-a reținut că *în cursul lunii decembrie 2018, inculpatul a creat pe un site de porno un profil cu numele persoanei vătămate B. P. A., pe care a postat mai multe fotografii cu aceasta nudă şi un filmuleţ în care B. P. A. întreţinea relaţii sexuale cu el (primul act material). Totodată, inculpatul a creat un profil fals pe reţeaua de socializare Facebook cu numele persoanei vătămate B. P. A., de pe care i-a trimis martorului D. S. mai multe fotografii cu persoana vătămată dezbrăcată (al doilea act material), în ipostaze intime. Instanţa a apreciat că aceste fapte întrunesc elementele constitutive ale infracţiunilor de fals informatic în formă continuată şi de violare a vieţii private* [34].

Așadar, în contextul faptelor ce vizează deschiderea conturilor „false” pe rețelele de socializare trebuie analizată și incidența infracțiunii de fals informatic.

---

[2] Problematica definirii noțiunii de „pornografie” a fost descrisă, într-o manieră memorabilă, în opinia concurentă a judecătorului Stewart în cauza Jacobellis v. Ohio din 1964, caz examinat de Curtea Supremă a SUA. Acest judecător a menționat că nu ar putea da o definiție definitivă noțiunii de „pornografie”, „dar poate să o recunoască atunci când o vede”. Spre exemplu, a se vedea: GEWIRTZ, P. On „I Know It When I See It”. În: The Yale Law Journal, 1996, vol. 105, p. 1027. ISSN 0044-0094; OWENS, E. W., BEHUN, R. J., MANNING, J. C., and REID, R. C. The Impact of Internet Pornography on Adolescents: A Review of the Research. În: Sexual Addiction & Compulsivity, 2012, vol. 19, iss. 1-2, p. 103. ISSN 2692-9953.

[3] Conform art. 325 („Falsul informatic”) din Codul penal al României, fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoarea de la unu la 5 ani.

[4] Conform art. 260[5] („Falsul informatic”) din Codul penal al Republicii Moldova, introducerea, modificarea sau ștergerea ilegală a datelor informatice ori restricționarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice se pedepsesc cu amendă în mărime de la 1350 la 1850 unități convenționale sau cu închisoare de la 2 la 5 ani.

După această divagație, trebuie de remarcat că obținerea unor date (care permit identificarea persoanei) despre abonatul la servicii de Internet trebuie să se facă cu respectarea unor garanții.

O asemenea constatare derivă din cazul *Benedik v. Slovenia*. În acest caz, Curtea Europeană a reținut, în fapt, că în baza informațiilor privind schimbul de fișiere cu pornografie infantilă prin intermediul unui site web de schimb al documentelor *peer-to-peer*, poliția a solicitat, în lipsa unui ordin al tribunalului, ca un provider de Internet (ISP) să dezvăluie date referitoare la un utilizator a cărui adresă dinamică a Protocolului de Internet („IP") fusese înregistrată. ISP a oferit numele și adresa tatălui reclamantului, care era abonat la serviciul de Internet legat de respectiva adresă IP.

Ulterior, poliția a obținut un ordin judiciar care cerea ca ISP să dezvăluie atât informațiile personale și referitoare la trafic ale abonatului care avea legătură cu adresa IP în discuție. În această bază, a fost percheziționat domiciliul familiei reclamantului și au fost confiscate computere în care s-au găsit materiale pornografice care implicau minori. Reclamantul a fost găsit vinovat de comiterea infracțiunii de expunere, fabricare, posesie și distribuire de materiale pornografice.

Acesta s-a plâns fără succes în fața tribunalelor naționale că secretul corespondenței și alte mijloace de comunicare puteau fi suspendate în baza unui ordin al tribunalului și, prin urmare, orice informație obținută în mod ilegal trebuia exclusă din categoria probelor. În această privință, Curtea Constituțională a Sloveniei conchis că reclamantul, care nu și-a ascuns în vreun mod adresa IP prin care a accesat Internetul, s-a expus în mod conștient la public și, așadar, a renunțat la așteptarea legitimă la respectarea vieții sale private. Prin urmare, deși informațiile privind identitatea utilizatorului adresei IP erau protejate ca fiind confidențiale în baza Constituției Sloveniei, nu era cerută emiterea vreunui ordin de către tribunal în vederea dezvăluirii acestora în cazul reclamantului [35].

În drept, Curtea Europeană a examinat dacă, în circumstanțele cazului, este incident art. 8 din Convenție. Mai întâi de toate, Curtea a clarificat natura interesului în discuție. Potrivit Curții Europene, informațiile despre abonați legate de adresele IP dinamice speciale alocate la anumite momente constituiau, în principiu, date cu caracter personal. Mai mult, acestea nu erau disponibile pentru public și, așadar, nu puteau fi comparate cu informațiile identificate în tradiționala carte de telefoane sau în bazele de date publice cu numerele de înregistrare ale autovehiculelor. Pentru a identifica un abonat căruia i-a fost alocat, la un anumit moment, o adresă IP dinamică specială, ISP trebuia să acceseze date stocate referitoare la evenimente de telecomunicare speciale. Utilizarea unor asemenea date stocate putea da naștere, prin ea însăși, unor probleme legate de viața privată. Singurul scop pentru obținerea informațiilor despre abonați fusese identificarea unei persoane particulare care stătea în spatele conținutului colectat în mod independent ce dezvăluia datele pe care le distribuise. Informațiile despre asemenea activități angajau aspectul confidențialității din momentul în care erau atribuite unei persoane identificate sau identificabile. Prin urmare, ceea ce ar părea o informație marginală căutată de către poliție, în special numele și adresa unui abonat, trebuia tratat ca fiind legat în mod inextricabil de conținutul relevant preexistent care dezvăluia datele. A reține altfel ar însemna să negi protecția necesară a informațiilor care ar putea dezvălui o bună parte din activitatea online a unei persoane, inclusiv detalii semnificative despre interesele, convingerile sau modul ei intim de viață [36].

În continuare, Curtea Europeană a analizat dacă reclamantul fusese identificat prin măsura contestată. Ea a notat că reclamantul era utilizator al serviciilor de Internet în discuție prin intermediul computerului său de acasă, iar activitatea sa online fusese monitorizată de către poliție. Faptul că acesta nu era abonat personal la serviciile de internet nu a avut vreun efect în privința așteptărilor sale de respectare a vieții private, care fuseseră angajate în mod indirect, odată ce erau dezvăluite informațiile despre abonat legate de uzul său privat al Internetului [37].

Apoi, Curtea Europeană a pus sub lupa analizei faptul dacă reclamantul a avut o așteptare legitimă la respectarea vieții sale private. Sub acest aspect, Curtea a apreciat că în ciuda naturii accesibile publicului a rețelei de distribuire a fișierelor în discuție, reclamantul se aștepta, în mod subiectiv, ca activitatea sa să rămână una cu caracter privat și ca identitatea sa să nu fie dezvăluită. Faptul că acesta nu și-a ascuns adresa sa IP dinamică putea să nu fie decisiv în stabilirea caracterului rezonabil al așteptării sale la respectarea vieții private dintr-un punct de vedere obiectiv. Aspectul de anonimitate al confidențialității online era un factor important care trebuia avut în vedere într-o asemenea analiză. În particular, nu s-a susținut că reclamantul

și-a dezvăluit vreodată identitatea în prestarea activității online în discuție sau că era, de exemplu, identificabil de către providerul particular al site-ului web printr-un cont sau prin datele sale de contact. Activitatea online a reclamantului angajase, prin urmare, un mare grad de anonimitate, așa cum o confirma faptul că adresa IP dinamică atribuită, chiar dacă vizibilă pentru alți utilizatori ai rețelei, nu putea fi asimilată unui anumit computer vără verificarea de către ISP a datelor, ca urmare a unei cereri primite din partea poliției. În plus, Constituția Sloveniei garanta secretul corespondenței și al comunicărilor și cerea ca orice ingerință în acest drept să se bazeze pe ordinul unui tribunal. Prin urmare, nu se putea spune că așteptarea legitimă a reclamantului la respectarea vieții private cu privire la activitatea sa online nu era garantată sau că era nerezonabilă [38].

Din aceste rațiuni, Curtea Europeană a decis că interesul reclamantului de a-i fi protejată identitatea cu privire la activitatea sa online se încadra în câmpul de aplicare al noțiunii de „viață privată”. Prin urmare, articolul 8 din Convecție era aplicabil [39].

Cu privire la fondul cauzei, Curtea Europeană a notat că cererea poliției adresată ISP și utilizarea de către aceasta a informațiilor despre abonat care au condus la identificarea reclamantului a echivalat cu o ingerință în drepturile sale în baza articolului 8 din Convenție. Măsurile poliției au avut o oarecare bază în dreptul național. De vreme ce legislația relevantă nu era coerentă în privința nivelului de protecție acordat interesului la confidențialitate al reclamantului, Curtea s-a bazat pe interpretarea Curții Constituționale a Sloveniei, potrivit căreia dezvăluirea identității persoanei care comunica și a datelor referitoare la trafic reclama, în principiu, ordinul unui tribunal. Cu privire la poziția Curții Constituționale a Sloveniei potrivit căreia reclamantul a renunțat la așteptarea sa legitimă la respectarea vieții private, Curtea nu a considerat-o reconciliabilă cu câmpul de aplicare al dreptului la respectarea vieții private în baza Convenției. Prin urmare, în acest caz era necesar ordinul unui tribunal și nimic din dreptul național nu împiedica poliția să-l obțină [40].

În opinia Curții Europene, invocarea prevederilor Legii privind procedura penală a Sloveniei (CPA) de către autoritățile naționale, lege care se referea la cererea de oferire a informațiilor despre deținătorul sau despre utilizatorul anumitor mijloace de comunicare electronică și care nu conținea reguli speciale cu privire la asocierea dintre adresa IP dinamică și informațiile privind abonatul, fusese, așadar, nepotrivită în mod manifest. Mai mult, ea nu oferea, în realitate, nicio protecție față de ingerințele arbitrare. La momentul de timp relevant, se pare că nu existau reglementări care să specifice condițiile pentru retenția datelor obținute în baza CPA și nici garanții împotriva abuzului funcționarilor statali în procedura de acces la și de transfer al unor asemenea date. Mai mult, nu exista niciun control independent al utilizării acestor competențe ale poliției, în ciuda faptului că aceste competențe obligau ISP să recupereze datele stocate privind conectarea și îi permiteau poliției să asocieze o mare parte din informațiile privind activitatea online cu o anumită persoană, fără consimțământul acesteia [41].

În concluzie, Curtea a conchis că legea pe care se baza măsura contestată și modul în care a fost aplicată aceasta de către tribunalele naționale erau lipsite de claritate și nu ofereau garanții suficiente împotriva ingerinței arbitrare. Așadar, ingerința în dreptul reclamantului la respectarea vieții sale private nu a fost „prevăzută de lege” și, prin urmare, a existat o încălcare a art. 8 din Convenție. Iar constatarea unei încălcări a constituit, în sine, o satisfacție echitabilă suficientă pentru prejudiciul moral solicitat de către reclamant [42].

Așadar, mesajul Curții Europene din cazul *Benedik v. Slovenia* a fost unul clar și răspicat: faptul persoana nu și-a ascuns adresa sa IP dinamică nu înseamnă că a renunțat la confidențialitatea datelor sale. Corelativ, furnizorii de Internet trebuie să dezvăluie date referitoare la utilizatorii/abonații săi în baza unei autorizații judecătorești. Consider că aici este importat ca să existe un control judecătoresc, care poate fi *ex-ante* sau, după caz, *ex-post*. Controlul judecătoresc trebuie să cenzureze orice pretins abuz.

Alte garanții au fost identificate de către Curtea Europeană în cazul *Breyer v. Germania*, deși într-un alt context (*i.e.*, cazul a vizat obligația legală a furnizorilor de servicii de a stoca datele cu caracter personal ale utilizatorilor de cartele pre-pay de telefonie mobilă și de a le pune, la cerere, la dispoziția autorităților). Printre asemenea garanții se numără: durata limitată de timp a stocării datelor (un an calendaristic de după anul în care lua sfârșit relația contractuală); solicitările de obținere a informațiilor erau permise atunci când se considerau necesare „pedepsirea faptelor cu caracter penal și contravențional, evitarea pericolelor și efectuarea de sarcini legate de securitate”; caracterul limitat al informațiilor furnizate (datele stocate se limitau la informațiile necesare pentru identificarea clară a abonatului relevant – numele și prenumele, adresa

și data de naștere); înregistrarea solicitărilor și a informațiilor furnizate în vederea supravegherii datelor cu caracter personal; analiza admisibilității transmiterii de date atunci când se găsesc motive pentru aceasta; posibilitatea de a cere despăgubiri în caz de încălcare a unor prevederi [43].

Spre deosebire de cazul *Benedik v. Slovenia*, în *Breyer v. Germania* Curtea Europeană nu a considerat o problemă faptul că transmiterea datelor putea fi cerută de mai multe autorități publice fără o autorizație a judecătorului și fără să fie nevoie de notificarea persoanelor vizate. Dar nu trebuie de făcut abstracție de faptul că circumstanțele acestor două cauze erau diferite. Acolo unde circumstanţele sunt diferite, este firesc ca soluția să fie tot diferită.

În cazul Republicii Moldova, din analiza art. 132^2 alin. (1) pct. 1) lit. h) și pct. 2) lit. a) din Codul de procedură penală rezultă că colectarea informației de la furnizorii de servicii de comunicații electronice se face cu autorizarea judecătorului de instrucţie. În contrast, identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic se face cu autorizarea procurorului. Solicitarea datele de identificare a persoanei care a acționat pe Internet în anonimat în baza unei autorizații a procurorului va veni în contradicție cu raționamentele din cazul *Benedik v. Slovenia*. În astfel de cazuri, trebuie aplicată direct Convenția și, respectiv, jurisprudența Curții Europene. Așa cum a afirmat lordul Bingham, „sarcina instanțelor este să țină pasul cu jurisprudența Strasbourg-ului, așa cum evoluează ea în timp: nu mai mult, însă cu siguranță nu mai puțin” [44]. Vreau să cred că așa vor face autoritățile noastre.

Concluzii

„Cât valorează un nume?”, a întrebat lordul Roger, de o manieră memorabilă, deși într-un alt context, în cazul *In re Guardian News and Media Ltd*, înainte de a-și răspunde la întrebare, la § 63, în termenii următori:

„Foarte mult, ar răspunde presa. Asta pentru că povestirile despre persoane cunoscute sunt mai atractive pentru cititori decât cele despre persoanele neidentificate. Nimic altceva decât natura umană. Și iată de ce, bineînțeles, chiar atunci când prezintă informații despre dezastrele grave, jurnaliștii caută, de obicei, subiecte despre cum au fost afectate persoanele private. Captarea atenției cititorilor prin povestirile scrise ține de tehnica prezentării, iar Curtea Europeană subliniază că articolul 10 [din Convenția Europeană a Drepturilor Omului] nu protejează doar substanța ideilor și a informațiilor, ci și forma în care sunt comunicate acestea (...). Nu este doar o chestiune de deferență manifestată față de independența editorială. Judecătorii recunosc faptul că redactorii știu mai bine cum să-și prezinte marfa de o manieră care va provoca interesul cititorilor publicației lor și care îi va ajuta astfel să asimileze informațiile. Obligaţia de a le comunica într-o formă abstractă, austeră, lipsită de o mare parte din interesul său pur omenesc, ar putea foarte bine să conducă la două efecte: comunicarea să nu fie citită, iar informațiile să nu fie transmise. În fine, o asemenea abordare ar putea ameninţa viaţa ziarelor şi a revistelor, care pot să informeze publicul doar dacă atrag suficienţi cititori şi doar dacă fac destui bani pentru a-şi continua activitatea” [45].

Ajustând aceste idei la tema analizată, pot afirma că un nume valorează mult pentru victimă și, respectiv, pentru autorități, astfel încât să se facă dreptate. Anonimitate pe Internet nu trebuie să constituie un obstacol pentru aflarea adevărului și, respectiv, pentru înfăptuirea justiției.

Așadar, persoanele care comit fapte prejudiciabile prin intermediul tehnologiilor informaționale trebuie identificate și diferite justiției. Ele nu pot rămâne *ingonito*. Identificarea persoanei care a comis o faptă prejudiciabilă reprezintă un element important pentru a aprecia caracterul „efectiv” al anchetei. Obligația de a efectua o anchetă efectivă este una de mijloace, nu de rezultat. Această obligație pozitivă a statului derivă din mai multe drepturi fundamentale garantate de Constituție și de Convenția Europeană a Drepturilor Omului (*e.g.*, dreptul la viață privată).

Este adevărat că persoana care a acționat în anonimat pe Internet are dreptul la confidențialitate, în special, la respectarea datelor cu caracter personal. Acest drept este garantat, între altele, de art. 28 din Constituție și de art. 8 din Convenția Europeană a Drepturilor Omului. Totuși, acest drept nu este absolut. El poate fi restrâns, desigur, dacă restrângerea/ingerința este prevăzută de lege, urmărește un scop legitim și este proporţională. Așadar, oricât de important ar fi, anonimatul pe Internet trebuie să se concilieze cu alte imperative. Unul din astfel de imperative îl constituie prevenirea infracțiunilor sau protecția drepturilor și libertăților altora.

Prin urmare, identificarea persoanei în vederea deferirii justiţiei are o pondere mai mare decât respectarea confidențialității pe Internet. Eșecul autorităților de a întreprinde măsuri de identificare a persoanei care a acționat pe Internet în anonimat poate conduce la o încălcare a Constituției și a Convenției Europene a Drepturilor Omului (*e.g.*, *Straistă v. Republica Moldova*). Faptul că o persoană care a acționat pe Internet în anonimat nu și-a ascuns adresa IP dinamică a dispozitivului nu înseamnă că ea a renunțat la protecția confidențialității datelor sale cu caracter individual (numele, prenumele, data și anul nașterii etc.).

În cele din urmă, furnizarea datelor de identificare a persoanei care a acționat pe Internet în anonimat trebuie să se facă cu respectarea anumitor garanții, în special, să se facă în baza unei autorizații a judecătorului. Acesta este standardul care derivă jurisprudența Curții Europene a Drepturilor Omului (*i.e.*, *Benedik v. Slovenia*) și de care trebuie să se ghideze autoritățile din Republica Moldova (și nu doar).

Referințe:

1. LUSTHAUS, J. *Cybercrime: The Industry of Anonymity*. PhD Thesis. University of Oxford, Oxford, 2016. [Accesat: 06.06.2023] Disponibil: https://bit.ly/3PEIj7B
2. UNODC. *Obstacles to cybercrime investigations.* [Accesat: 06.06.2023] Disponibil: https://bit.ly/3V6MzOe
3. XINGAN, L. *Phenomenal Exploration into impact of Anonymity on Law and order in Cyberspace.* [Accesat: 06.06.2023] Disponibil: https://bit.ly/3PtX2SR
4. *Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology adopted on 11 September 1995.* [Accesat: 06.06.2023] Disponibil: https://bit.ly/3FyKZir
5. *Convention of the Council of Europe on Cybercrime, Budapest, 23.XI.2001.* [Accesat: 06.06.2023] Disponibil: https://rm.coe.int/1680081561
6. *Legea nr. 6 din 2 februarie 2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică*. În: *Monitorul oficial al Republicii Moldova*, 2009, nr. 37-40.
7. SEGER, A. *A New Protocol to the Convention on Cybercrime: For a more effective criminal justice response to crime online ─ with strong safeguards.* [Accesat: 06.06.2023] Disponibil: https://bit.ly/3huhdn7
8. *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*. [Accesat: 06.06.2023] Disponibil: https://bit.ly/3Yr0mlH
9. *Legea nr. 20 din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice*. În: *Monitorul oficial al Republicii Moldova*, 2010, nr. 11-12.
10. RENIȚĂ, Gh. *Controverse legate de răspunderea penală pentru manipularea unui eveniment și pariurile aranjate săvârșite în cyberspațiu.* În: *Studia Universitatis Moldaviae, Seria Ştiinţe Sociale*, 2017, nr. 8(108), p. 239. ISSN 1814-3199.
11. *Case of T.M. and C.M. v. the Republic of Moldova, Application no. 26608/11, Judgment of 28 January 2014, § 38.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-140240
12. *Case of Dornean v. the Republic of Moldova, Application no. 27810/07, Judgment of 29 May 2018, § 38.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-183203
13. SHINDER, D. L. *Online anonymity: Balancing the needs to protect privacy and prevent cybercrime*. [Accesat: 06.06.2023] Disponibil: https://tek.io/3BHj52K
14. *Case of K.U. v. Finland, Application no. 2872/02, Judgment of 2 December 2008, §§ 7-14, § 40*. [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-89964
15. *Ibidem*, § 46.
16. *Ibidem*, § 47.
17. *Ibidem*, § 48.
18. *Ibidem*, § 49.
19. *Case of Karttunen v. Finland, Application no. 1685/10, Decision, 10 May 2011.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-104816
20. ALEXY, R. *Formula cântăririi.* În: *Noua revistă de drepturile omului*, 2019, nr. 1, p. 97. ISSN 1841-4710.
21. ALEXY, R. *Demnitatea umană și analiza proporționalității.* În: *Noua revistă de drepturile omului*, 2017, nr. 4, p. 87. ISSN 1841-4710.

22. *Ibidem.*
23. ALEXY, R., *Formula cântăririi*, p. 98.
24. ALEXY, R., *Demnitatea umană și analiza proporționalității*, p. 87.
25. BARAK, A. *Proportionality Constitutional Rights and their Limitations.* New York: Cambridge University Press, 2012, p. 350. ISBN 9781107401198.
26. SINCLAIR-BLAKEMORE, A. *Cyberviolence Against Women Under International Human Rights Law: Buturugă v Romania and Volodina v Russia (No 2)*. În: *Human Rights Law Review,* 2023, vol. 23, iss. 1, pp. 1-27. ISSN 1461-7781.
27. *Case of Volodina v. Russia (no. 2), Application no. 40419/19, Judgment of 14 September 2021, § 68, § 20.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-211794
28. *Case of Straistă v. the Republic of Moldova, Application no. 14191/14, Judgment of 15 March 2022, § 2*. [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-216169
29. *Ibidem*, § 9.
30. *Sentința Judecătoriei Chișinău (sediul Buiucani) din 27 aprilie 2018. Dosarul nr. 1-1254/2017*. [Accesat: 06.06.2023] Disponibil: https://shorturl.at/bnxz4
31. BRÎNZĂ, S., STATI, V. *„Sexting", „sextorsion", „revenge porn": fenomene reflectate în Codul penal al Republicii Moldova?* În: *Studia Universitatis Moldaviae, Seria „Științe sociale"*, 2021, nr. 3, pp. 3-17. ISSN 1814-3199.
32. *Ibidem.*
33. *Decizia nr. 4 din 25 ianuarie 2021 a Înaltei Curți de Casație și Justiție a României.* [Accesat: 06.06.2023] Disponibil: https://www.iccj.ro/2021/01/25/decizia-nr-4-din-25-ianuarie-2021/
34. *Apud: Decizia nr. 4 din 25 ianuarie 2021 a Înaltei Curți de Casație și Justiție a României.* [Accesat: 06.06.2023] Disponibil: https://www.iccj.ro/2021/01/25/decizia-nr-4-din-25-ianuarie-2021/
35. *Case of Benedik v. Slovenia, Application no. 62357/14, Judgment of 24 April 2018, §§ 7-29.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-182455
36. *Ibidem*, § 108-110.
37. *Ibidem*, § 111-114.
38. *Ibidem*, § 115-118.
39. *Ibidem*, § 119.
40. *Ibidem*, § 127-128.
41. *Ibidem*, § 129-132.
42. *Ibidem*, § 133-134, § 138.
43. *Case of Breyer v. Germany, Application no. 50001/12, Judgment of 30 January 2020.* [Accesat: 06.06.2023] Disponibil: https://hudoc.echr.coe.int/?i=001-200442
44. *Apud: Lordul David NEUBERGER. „Cât valorează un nume?" – Viața privată și discursul anonim pe Internet, Idei-cheie ale Conferinței 5RB, 30 septembrie 2014.* În: *Noua revistă de drepturile omului*, 2014, nr. 2, p. 99. ISSN 1841-4710.
45. *Apud: § 29 din Hotărârea Curții Supreme a Regatului Unit din 19 iulie 2017 în cazul Khuja (recurent) v. Times Newspapers Limited și alții (intimați)*. [Accesat: 06.06.2023] Disponibil: https://shorturl.at/hELT8

Notă: *acest articol a fost elaborat în cadrul proiectului „Consolidarea capacității Republicii Moldova în combaterea abuzului și exploatării sexuale online a copiilor".*

Date despre autor:
Gheorghe RENIȚĂ, doctor în drept, lector universitar, Facultatea de Drept, Universitatea de Stat din Moldova.
E-mail: gheorghe.renita@usm.md
ORCID: 0000-0003-2722-009X

Prezentat la 14.09.2023