ANALIZA PRACTICII INTERNAȚIONALE ÎN DOMENIUL ASIGURĂRII VIEȚII PRIVATE ÎN CONTEXTUL SECURITĂȚII CIBERNETICE

Virginia Zaharia,
doctor în drept, lector universitar,
Universitatea Cooperatist-Comercială din Moldova,
e-mail: virginica.zaharia@yahoo.com
0000-0002-4822-026X

Ala Luca,
doctor în drept, lector universitar,
Universitatea Cooperatist-Comercială din Moldova
e-mail: lucaala@mail.ru

Abstract. Analyzing the proposed research topic on the Internet and the protection of fundamental rights in this area, we argue that the Internet is currently a machine that can lead to modernization and change in society provided that human rights are respected, and therefore we need international guidance. , national legislation, data security and freedom on the other hand, and this study of international jurisprudence will give us the opportunity to examine several cases of human rights violations through the Internet.Being a strong and weakest link, Cybersecurity needs increased attention to implement a strategic culture common to all states of the world and to develop and implement national cyber security strategies to meet the challenges of integrity protection. increase the effectiveness and safe functioning of critical and political cybersecurity infrastructures, must provide a secure and reliable digital environment based on the protection and preservation of freedoms and respect for human rights online, in particular the protection of privacy and security. of personal data.

Keywords: European Convention on Human Rights, European Court of Human Rights, case law, privacy, cyber security, Internet, case, practice, online, human rights, fundamental.

Rezumat. Analizând subiectul propus spre cercetare privind Internetul și protecția drepturilor fundamentale în acest spațiu, susținem că Internetul actualmente este un utilaj care poate duce la modernizarea și schimbarea în societate cu condiția de a respecta drepturile omului, și de aceea avem nevoie de o orientare la nivel internațional, acte normative la nivel național, siguranța datelor și libertatea pe de altă parte, iar acest studiu a jurisprudenței internaționale ne va oferi posibilitatea de a examina mai multe cazuri vizând încălcarea drepturilor omului prin intermediului Internetului. Fiind o verigă solidă și totodată cea mai slabă, Securitatea Cibernetică necesită o atenție sporită care necesită de a implementa o cultură strategică comună tuturor statelor lumii și de a elabora și implementa strategii naționale a securității cibernetice comune pentru a putea face față sfidărilor, pentru protecția integrității fizice a cetățenilor, prin sporirea eficienții eficacității și funcționării sigure a infrastructurilor critice și politice de securitate cibernetică, trebuie să ofere un mediu digital sigur și fiabil bazat pe protecția și conservarea libertăților și pe respectarea drepturilor omului on-line, în special protecția vieții private și a datelor cu caracter personal.

Cuvinte-cheie: Convenția Europeană a Drepturilor Omului, Curtea Europeană a Drepturilor Omului, jurisprudență, viață privată, securitate cibernetică, Internet, cauză, practica, online, drepturile omului, fundamental.

JEL: K24, K10, K15

Introducere. Analizând subiectul ce vizează Internetul și protecția drepturilor fundamentale în acest spațiu, susținem că Internetul actualmente este un utilaj care poate duce la modernizarea și

schimbarea în societate cu condiția de a respecta drepturile omului, și de aceea avem nevoie de o orientare la nivel internațional, acte normative la nivel național, siguranța datelor și libertatea pe de altă parte. Cu toate acestea multe state îngrădesc cetățenilor săi accesul la Internet și aceasta duce la încălcarea drepturilor omului și proprietății intelectuale ceea ce este inadmisibil, deoarece libertatea vieții private pe Internet se poate realiza pe baza principiului drepturilor omului și buna guvernare. Spre deosebire de alte mijloace de comunicare, cum ar fi radio, televiziune și publicații, bazate pe transmiterea de informații, Internetul reprezintă un progres semnificativ față de interactivitate.

Multe persoane percep o amenințare la adresa vieții private, deoarece colectarea pe scară largă a datelor cu caracter personal prin intermediul internetului, și necunoașterea scopul utilizării lor care cu toate aceste reprezintă un domeniu protejat, oricum este un moment de îngrijorare.

Fiind vorba despre o temă în curs de dezvoltare, acest studiu a jurisprudenței internaționale ne va oferi posibilitatea de a examina mai multe cazuri vizând încălcarea drepturilor omului prin intermediului Internetului. Vor fi analizate cazuri care vizează următoarele subiecte:

1. Internetul şi protejarea sau păstrarea datelor (protejarea datelor cu caracter personal de către stat sau de către furnizorii accesului la Internet, probleme ridicate de stocarea de date, Facebook, cazul deosebit al minorilor în acest context/garanţiile procedurale şi condiţiile care se aplică cererilor de anchetă în materie de criminalitate informatică (articolul 15 din Convenţia de la Budapesta asupra criminalităţii informatice);
2. Internetul şi libertatea de exprimare (de exemplu drepturile persoanelor care folosesc Internetul în scop de satiră sau de critică/violenţele împotriva copiilor/garanţiile procedurale şi condiţiile care se aplică la cererilor de anchetă în materie de criminalitate informatică (art.15 din Convenţia de la Budapesta asupra criminalităţii informatice);
3. Internetul şi drepturile de proprietate intelectuală;
4. Dreptul de acces la Internet (dreptul la pregătire pe Internet, ucenicia Internetului pentru copii, accesul pentru deţinuţi, obligaţiile pozitive ce revin statelor ce blochează sau filtrează site-urile, tăierea accesului la Internet);
5. Protecţia oferită de către stat împotriva prejudiciilor pe care le pot provoca activităţile infracţionale pe Internet (obligaţiile de a lua măsuri pozitive pentru a proteja individul împotriva încălcărilor dreptului la viaţa privată / obligaţia de a proteja individul (mai ales copiii, în special în cazul violenţelor sexuale) de persoanele care participă la activităţi extremiste, difuzând pornografie sau apărând violenţa sau alte acţiuni interzise prin lege / garanţiile procedurale şi condiţiile care se aplică cererilor de anchetă în materie de criminalitate informatică (articolul 15 din Convenţia de la Budapesta asupra criminalităţii informatice) [21].

Rezultate și discuții. Trebuie de remarcat, că cuvântul "jurisdicţie" se defineşte în principal prin capacitatea unei instanţe judiciare de a analiza o cauză şi a o soluţiona sau de a lua anumite decizii în această privinţă. Cu toate acestea, acest cuvânt desemnează adesea şi circumscripţia teritorială a aceleiaşi instanţe. Este util de reamintit în această privinţă că, fiind un atribut al suveranităţii statului, jurisdicţia se limitează, în principiu, la teritoriul acestuia [13, p.213].

De asemenea,este important de înţeles ce fel de "probleme legate de jurisdicţie" sunt ridicate în cauzele privind Internetul. Aşa cum a fost deja remarcat, jurisdicţia este, în principiu, teritorială. Or, tranzacţiile şi publicaţiile pe Internet pot depăşi frontierele. Cu alte cuvinte, cauzele referitoare la Internet prezintă, în cea mai mare parte a timpului, un element de extranietate. Astfel, se pune în special problema circumstanţelor în care un tribunal îşi poate exercita jurisdicţia atunci când o parte pârâtă se află sau domiciliază într-o altă ţară decât cea în care este citată pentru un delict civil sau penal care ar fi fost comis pe Internet [10].

Totuşi este vorba, în principal, de o chestiune care trebuie soluţionată de instanţele interne după unul din principiile de drept internaţional privat aplicabile în materie de jurisdicţie. Curtea Europeană pentru Drepturile Omului nu trebuie să examineze direct această chestiune. De altfel, a confirmat acest

lucru în Hotărârea recentă *Premininy împotriva Rusiei* (nr. 44973/04, 10 februarie 2011) [18]. Reclamanţii, doi cetăţeni ruşi domiciliaţi în Rusia, au fost deţinuţi în această ţară pe motiv că erau bănuiţi că au piratat, în anul 2001, sistemul de securitate online al băncii americane *"Green Point Bank",* că i-au sustras baza de date cu clienţi şi că au extorcat bani de la ea în schimbul promisiunii de a nu publica conţinutul acestei baze de date pe Internet. Primul reclamant s-a considerat victima abuzurilor în arest preventiv şi a susţinut că cererea sa de punere în libertate nu a făcut obiectul unei analize efective. Cauza a fost soluţionată de tribunalele ruseşti care s-au considerat competente. Deoarece nimeni nu a pledat în faţa ei incompetenţa judecătorului rus de a examina cauza, Curtea s-a mulţumit să statueze asupra cererilor pe care reclamanţii, în faţa ei, cu privire la detenţie, le-au întemeiat pe articolele 3 şi 5 din Convenţie, fără să evoce mai departe problema jurisdicţiei. Este important de reamintit, în această etapă, că Curtea nu-şi va exercita propria "jurisdicţie" decât dacă se va putea stabili că încălcarea invocată într-un anumit caz este în vreun fel atribuibilă unui stat parte la Convenţie şi că ţine de jurisdicţia acestuia din urmă, fără care cererea va fi respinsă pentru incompatibilitate ratione personae sau ratione loci. Jurisprudenţa tradiţională a Curţii asupra excepţiilor de inadmisibilitate *ratione personae* sau *ratione loci* va putea deci fi inclusă, pe viitor, în cauzele privind Internetul.

a) Domeniul de aplicare al articolului 8 al CEDO şi datele cu caracter personal. Convenţia Consiliului Europei din 1981 pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal le defineşte pe acestea drept orice informaţie privind o persoană fizică identificată sau identificabilă.Protejarea şi păstrarea datelor cu caracter personal sunt clar legate de dreptul la viaţa privată aşa cum este garantat de articolul 8 din Convenţie. Această ultimă dispoziţie apără o întreagă serie de drepturi, şi anume dreptul la respectarea vieţii private şi de familie, a domiciliului şi corespondenţei. Curtea a considerat, de altfel, că protejarea datelor cu caracter personal joacă un rol fundamental în exercitarea dreptului la respectarea vieţii private şi de familie (*S şi Marper împotriva Regatului Unit al Marii Britanii [GC] nr. 30562/04 şi 30566/04, alin. 103, 4 decembrie 2008*) [19]. Dreptul la viaţa privată include confidenţialitatea comunicărilor, inclusiv cele ale schimburilor prin poştă, telefon, mesagerie electronică şi prin alte mijloace de comunicare, precum şi confidențialitatea informaţiilor, inclusiv, după toate aparenţele, cea a accesului la Internet.

Noţiunea de viaţă privată cuprinde elemente care se raportează la dreptul la imagine al unei persoane (*Sciacca împotriva Italiei, nr. 50774/99, alin. 29, CEDO 2005-I*) [20]. Cu alte cuvinte, fotografiile sau videogramele în care se arată imaginea unei persoane ţin de domeniul de aplicare al articolului 8. Trebuie să se ţină cont de el atunci când este în discuţie păstrarea imaginilor pe site-urile de Internet comune sau de socializare. Înregistrarea vocii unei persoane în vederea analizării acesteia reprezintă de asemenea un amestec în dreptul la respectarea vieţii sale private (*P.G. şi J.H. împotriva Regatului Unit al Marii Britanii, nr. 44787/98, alin. 59-60, CEDO 2001-IX*) [15].

Publicarea datelor sau informaţiilor strânse în locurile publice prin mijloace sau într-o măsură care depăşeşte ceea ce este în mod normal previzibil poate include de asemenea aceste materiale în domeniul de aplicare al articolului 8 par. 1 (*Peck împotriva Regatului Unit al Marii Britanii, nr. 44647/98, alin. 60-63, CEDO 2003-I,* privind transmiterea mediilor audiovizuale, în scopul difuzării, de imagini video ale reclamantului înregistrate într-un loc public) [16].

Dacă articolul 8 are drept obiect în principal protejarea individului împotriva amestecurilor arbitrare ale puterilor publice, la aceasta se pot adăuga obligaţii pozitive inerente respectării efective a vieţii private sau de familie (*Airey împotriva Irlandei, 9 octombrie 1979, alin. 32, seria A nr. 32*) [4]. Aceste obligaţii pot implica adoptarea de către stat de măsuri vizând respectarea vieţii private până la relaţiile indivizilor între ei, de exemplu un internaut şi persoanele care permit accesul la un site privat de Internet. Altfel spus, statului îi revine obligaţia pozitivă de a lua măsurile vizând prevenirea efectivă a acţiunilor ce aduc atingere gravă datelor privind o persoană, deseori prin intermediul dispoziţiilor

penale eficiente (*X şi Y împotriva Olandei 26 martie 1985, alin. 23-24 şi 27, seria A nr. 91* [23]*; August împotriva Regatului Unit al Marii Britanii (decizie), nr. 36505/02, 21 ianuarie 2003* [6]*; şi M.C. împotriva Bulgariei, nr. 39272/98, alin. 150, CEDO 2003-XII*) [11].

Cauza *K.U. împotriva Finlandei* (nr. 2872/02, alin. 43, 02 decembrie 2008) [9], scoate în evidenţă această obligaţie pozitivă în cadrul unei plângeri legate de Internet. În privinţa Internetului, răspunderea statului poate fi angajată fără îndoială prin fapta terţilor care păstrează datele pentru particulari. Strângerea, păstrarea, utilizarea şi comunicarea de către stat a datelor cu caracter personal, de exemplu într-un fişier al poliţiei, implică amestecul în dreptul la respectarea vieţii private a fiecăruia, aşa cum este el garantat de articolul 8 paragraful 1 din Convenţie (*Leander împotriva Suediei, 26 martie 1987, alin. 48, seria A nr. 116*) [2].

În cauza *Copland împotriva Regatului Unit al Marii Britanii* [7], citată anterior, problema supravegherii folosirii telefonului, e-mail-ului şi Internetului a fost discutată în temeiul art.8. În Hotărârea sa, Curtea a considerat nesemnificativ faptul că informaţiile deţinute de colegiu sau de reclamantă spre a fi folosite, nu au fost nici divulgate nici reţinute împotriva sa în cadrul unei proceduri disciplinare sau în cadrul altei proceduri. Simpla păstrare a informaţiilor aducea atingere vieţii sale private. Curtea nu exclude faptul că supravegherea folosirii din partea unui angajat a telefonului, a e-mail-ului sau a Internetului la locul de muncă ar putea fi considerată "necesară într-o societate democratică" în anumite cazuri, prin urmare că este urmărit un scop legitim. Cu toate acestea, în această cauză, nicio lege nu reglementa supravegherea în momentul comiterii faptelor.

În Hotărârea *K.U. împotriva Finlandei* [9], citată anterior, Curtea a hotărât că, chiar dacă libertatea de exprimare şi confidenţialitatea comunicărilor sunt preocupări primordiale şi utilizatorii telecomunicaţiilor şi ai serviciilor de Internet trebuie să aibă garanţia că le sunt respectate intimitatea şi libertatea de exprimare, această garanţie nu poate fi absolută şi uneori trebuie să dispară în faţa altor imperative legitime cum ar fi apărarea ordinii şi prevenirea infracţiunilor penale sau apărarea drepturilor şi libertăţilor altuia.

b) Internetul si Dreptul la Libertatea de Expresie. Libertatea de exprimare este garantată de articolul 10 din CEDO.Libertatea de exprimare protejată de art.10, alin. 1 constituie unul din fundamentele esenţiale ale unei societăţi democratice (de exemplu *Handyside împotriva Regatului Unit al Marii Britanii*, 7 decembrie 1976, seria A nr. 24) [8]. Restricţiile acestei libertăţi prevăzute la art.10, alin. 2 sunt de o interpretare riguroasă. Amestecurile în exercitarea acestei libertăţi de către state sunt posibile cu condiţia să fie "necesare într-o societate democratică", şi anume, potrivit jurisprudenţei CtEDO, să corespundă unei "nevoi sociale imperioase", să fie proporţionale cu scopul legitim urmărit în temeiul par. 2 al art.10 şi justificate prin hotărâri judecătoreşti motivate în mod pertinent şi suficient. Dacă autorităţile naţionale dispun de o anumită marjă de apreciere, aceasta nu este nelimitată, deoarece se îmbină cu un control european din partea Curţii (*Alexei Ovchinnikov împotriva Rusiei, nr. 24061/04, par. 51, 16 decembrie 2010*) [5].

Măsurile de blocare a unor site-uri *WEB* prin intermediul furnizorilor de servicii internet, constituie o măsură de cenzură a conținutului media online, măsură ce ridică probleme serioase în ceea ce privește respectarea drepturilor omului. Un caz recent este decizia *Yildirim c. Turciei* (Cererea nr. 3111/10), pronunțată pe 18 decembrie 2012 [1], CtEDO a stabilit ca Turcia a încălcat art.10 al CEDO, în urma deciziei unei instanțe de a bloca accesul la toate paginile de internet găzduite de Google pe teritoriul Turciei. Reclamantul a invocat faptul că i-a fost cenzurat dreptul de a accesa propria pagină de internet, găzduită de Google, ca urmare a unei ordonanțe dată într-o cauză penală care nu avea nicio legătură cu el sau cu site-ul. Ordonanța fusese dată în cazul proprietarului unui blog găzduit de Google care era urmărit penal pentru ca insultase memoria lui Atatürk pe blogul său. Ca rezultat al acestei ordonanțe, accesul la toate celelalte bloguri găzduite de Google a fost blocat de către Directoratul pentru Telecomunicații (TİB). TİB a solicitat instanței să procedeze astfel, argumentând ca aceasta era singura soluție din punct de vedere tehnic pentru a bloca accesul la site-ul incriminat, dat fiind faptul

ca proprietarul său locuia în străinătate. Reclamantul nu a avut acces la propria pagina de internet nici după ce procesul proprietarului site-ului incriminat a încetat fără să fi fost soluționat, întrucât autoritățile nu au reușit să îl identifice. CtEDO a reiterat că art.10 se aplică nu doar conținutului informației, ci și mijloacelor de diseminare a acesteia. Curtea a considerat că efectele ordonanței semnifică "o restricție a accesului la internet", „care a devenit în prezent unul dintre principalele mijloace ale exercitării dreptului la libertatea de exprimare și la informare". În acest caz Curtea a reținut ca Legea nr. 5651 prevedea blocarea accesului la conținutul publicat pe internet dacă exista suficiente motive pentru ca acesta să fie suspectat ca ar atrage o pedeapsă penală. Cu toate acestea, nici Google, nici reclamantul nu erau părți în cauza respectivă. Legea nu face nicio referire la blocarea în întregime a accesului la un furnizor de servicii de găzduire, precum Google. În plus, decizia blocării la scară largă a fost luată fără ca instanța să aplice un test al proporționalității și să se asigure ca efectele dorite nu puteau fi obținute printr-o măsură mai puțin restrictivă [1].

În jurisprudența CtEDO mai există 3 cazuri privind limitarea dreptului la exprimare în ce privește publicațiile pe internet, care ulterior v-or fi supuse analizării.

În cazul *K.U. împotriva Finlandei*, CtEDO consideră că în pofida faptului că libertatea de exprimare şi confidenţialitatea comunicărilor sunt preocupări primordiale şi chiar dacă utilizatorii telecomunicaţiilor şi ai serviciilor de Internet trebuie să aibă garanţia că le sunt respectate intimitatea şi libertatea de exprimare, această garanție nu poate fi absolută şi uneori trebuie să dispară în faţa altor imperative legitime cum ar fi apărarea ordinii şi prevenirea infracţiunilor penale sau apărarea drepturilor şi libertăţilor altuia. (*K.U. împotriva Finlandei*) [9].

În cazul *Times Newspapers Ltd c.Marea Britanie* (1 şi 2) [22], CtEDO a declarat că: "Cu accesibilitatea lor și capacitatea lor de a reține și de a distribui cantități mari de date, site-uri de pe Internet contribuie în mod semnificativ la îmbunătățirea accesului public la știri și în general pentru a facilita comunicarea informații. Crearea de arhive Internet reprezintă un aspect cheie al rolului jucat de site-uri, CtEDO consideră că se încadrează în domeniul de aplicare al articolului 10".

În cele din urmă, în cazul comitetului de redactare *Pravoye Delo și Shtekel c . Ucraina* [17], CtEDO a statuatcă: "Lipsa unui cadru legal adecvat pe plan intern care să permită jurnaliștilor să folosească informațiile de pe Internet, fără teama de a suporta sancțiuni împiedică grav exercitarea de către presa din rolul său vital de "câine pază" (watchdogging). Însă libertatea presei încetează atunci când nu vizează decât să satisfacă simpla curiozitate a anumitor cititori în detrimentul dreptului la respectarea vieţii private şi de familie. Astfel, o informaţie publicată deja pe Internet şi deci figurând în domeniul public – nu oferă presei dreptul absolut de a o reproduce. Presa nu trebuie să retransmită detalii asupra vieţii private sau de familie a unui individ care, deşi a fost postat pe Internet, nu se înscriu în nicio dezbatere publică sau politică pe o temă de importanţă generală.

c) Internetul și Proprietatea Intelectuală. Dreptul de proprietate intelectuală are drept obiect asigurarea apărării creaţiilor spirituale, indiferent de forma lor. Convenţia din 14 iulie 1967 de constituire a Organizaţiei mondiale a proprietăţii intelectuale formulează drepturile apărate de această noţiune: lucrările literare, artistice, interpretările, invenţiile, descoperirile ştiinţifice, desenele şi modelele, mărcile de fabrică, comerciale, de serviciu, etc. Astfel, sunt apărate nu numai ideile, ci şi forma de exprimare a ideii însăşi. Autorul unei creaţii spirituale dispune:

- pe de o parte, de un drept moral care îi permite să beneficieze de dreptul de divulgare a bunului; un terţ trebuie să obţină o permisiune din partea sa de a-l utiliza, de a-l reproduce, etc.;
- pe de altă parte, de un drept patrimonial care-i permite să-şi exploateze creaţia (cu prilejul unei interpretări, unei reproduceri, etc.).

În materie informatică, un program este legat de proprietatea intelectuală. Acelaşi lucru este valabil pentru întreaga creaţie (ca un articol, o imagine, sunete, etc.) creată pe computer. Elementul difuzat pe Internet poate constitui, de asemenea, intrinsec, obiectul unei protecţii (exemplul cărţii).

Jurisprudenţa CtEDO este relativ puţin informată în materie de proprietate intelectuală şi Internet. Se pot face totuşi constatările următoare.

O licenţă pentru furnizarea accesului la Internet. Aceasta constituie un "bun" (*Megadat.com SRL împotriva Moldovei*, nr. 21151/04, alin. 63, 8 aprilie 2008) [12]. În această cauză privind o societate care era cel mai mare furnizor de acces la Internet din Moldova, societatea reclamantă s-a plâns de rezilierea licenţelor sale de telecomunicaţii pe motiv că nu informase autoritatea de control competentă asupra unei schimbări de adresă. Ea susţinea, în plus, că a fost singura din 91 de societăţi care a fost pedepsită cu o sancţiune atât de dură. În consecinţă, societatea a fost constrânsă să-şi înceteze activitatea. CtEDO a reţinut că instanţele moldovene procedaseră la o examinare formalistă al cauzei, fără a pune în balanţă chestiunea generală în discuţie, pe de o parte şi sancţiunea impusă, pe de altă parte. Prin urmare, Curtea consideră că procedura era arbitrară şi că societăţii reclamante i s-a aplicat o măsură de o severitate disproporţionată. În plus, ţinând cont de tratamentul discriminatoriu al cărei obiect l-a făcut societatea reclamantă, Curtea a concluzionat că autorităţile nu urmaseră o politică coerentă hotărând să rezilieze licenţele societăţii Megadat.com SRL. Prin urmare, a avut loc încălcarea art.1 din Protocolul nr. 1.

d) Dreptul de acces la Internet. CtEDO nu a avut încă ocazia de a statua asupra unei plângeri întemeiate pe un refuz sau o limitare a accesului la Internet. Acestea fiind spuse, plângeri de acest gen au fost deja prezentate în temeiul art.10. În septembrie 2010, CtEDO a comunicat statului pârât plângerea unui deţinut lituanian bazată pe refuzul accesului la Internet spre a se înscrie la Universitate. În acelaşi an, mai multe plângeri au fost îndreptate împotriva Turciei cu privire la blocarea accesului la anumite site-uri de Internet în scopul combaterii criminalităţii şi apărării drepturilor autorului. În unul din aceste cazuri, site-ul de Internet al reclamantului a fost blocat pe motiv că era dificil din punct de vedere tehnic să fie separat de un alt site interzis de autorităţi. Într-un alt caz, reclamantul era un user al site-ului de Internet consacrat muzicii şi reţelelor de socializare. Aceste cauze au fost comunicate statului pârât în februarie 2011.

e) Protejarea comunicaţiilor pe Internet şi obligaţiile statelor. Obligaţia statelor de a prevedea o reglementare suficient de accesibilă şi clară. Supravegherea de către angajator a folosirii personale a conexiunilor la Internet fără ca angajatul său să ştie şi strângerea şi păstrarea datelor (site-uri vizitate, datele şi durata vizitelor), are legătură cu articolul 8. De altfel, angajatorul reclamantei fiind un organ public, chestiunea ridicată în cazul în speţă era raportată la obligaţia negativă ce îi revenea statului de a nu-i încălca viaţa privată. În ceea ce priveşte legalitatea acestui amestec, CtEDO afirmă în cauza *Copland împtriva Regatului Unit al Marii Britanii* [7], citată anterior, alin. 45-46 şi 48, că: potrivit jurisprudenţei constante, expresia "prevăzută de lege" implică – şi asta reiese din obiectul şi din scopul articolului 8 – că dreptul intern trebuie să ofere o anumită protecţie împotriva atingerilor arbitrare ale puterii publice aduse drepturilor garantate de paragraful 1. Este cu atât mai mult valabil atunci când sunt adoptate măsuri de supraveghere ca cele în cauză, dată fiind lipsa controlului public şi riscul abuziv de putere.

Această expresie nu numai că impune respectarea dreptului intern, ci priveşte şi calitatea legii, care trebuie să fie conformă principiilor ce caracterizează statul de drept. Pentru a îndeplini cerinţa de previzibilitate, legea trebuie să folosească termeni destul de clari pentru a indica tuturor în mod suficient în ce împrejurări şi în ce condiţii abilitează puterea politică să ia asemenea măsuri. Datorită lipsei la acea vreme a unui text de drept intern care să reglementeze măsurile de supraveghere, amestecul în cazul în speţă nu era "prevăzut de lege" aşa cum o impune art.8 par.2 din CEDO. CtEDO nu exclude faptul că supravegherea folosirii din partea unui angajat a telefonului, a poştei electronice sau a Internetului la locul de muncă ar putea fi considerată drept "necesară, într-o societate democratică" în anumite cazuri în care se urmăreşte un scop legitim. Cu toate acestea, ţinând cont de concluzia la care a ajuns, nu se poate pronunţa asupra acestei chestiuni în prezenta speţă.

În ceea ce priveşte caracterul suficient de accesibil al legii, Curtea consideră, în cauza *Perrin împotriva Regatului Unit al Marii Britanii* (decizie), că dacă administrarea site-ului de Internet corespunde practicării unei activităţi profesionale, se poate considera pe bună dreptate că trebuie făcută dovada unei mari prudenţe şi trebuie obţinute avizele juridice necesare.

f) Dificultăţile obiective, pe care mijloacele tehnice nu sunt întotdeauna în măsură să le depăşească.

În cauza *Muscio împotriva Italiei* (decizie), nr. 31358/03, din 13 noiembrie 2007 [14], preşedintele unei asociaţii de preoţi catolici, care a primit mesaje electronice nesolicitate ("*SPAM*") cu caracter pornografic, a contestat clasarea plângerii sale împotriva lui X. Curtea consideră că primirea de comunicări nedorite poate reprezenta un amestec în viaţa privată. Totuşi, utilizatorii poştei electronice, odată conectaţi la Internet, nu mai pot beneficia de o protecţie efectivă a vieţii lor private şi se expun primirii de mesaje nedorite, pe care le pot sorta prin folosirea de "filtre" informatice. Mai multe ţări şi mai mulţi operatori informatici întâlnesc dificultăţi obiective în combaterea fenomenului spam şi în accesul la expeditorii acestor mesage, pe care mijloacele tehnice nu sunt mereu în măsură să le depăşească. În aceste împrejurări, Curtea nu poate concluziona că statul ar fi trebuit, pentru a se achita de eventualele sale obligaţii pozitive ce decurg din articolul 8, să depună eforturi suplimentare [21].

De asemenea, în opinia sa: operatorii reţelei informatice acţionează în cadrul acordurilor cu autorităţile statului şi sub supravegherea acestora din urmă. Prin urmare, dacă a considerat că statului sau operatorului informatic la care s-a abonat se putea reproşa o greşeală pentru nesupravegherea şi/sau punerea la punct a sistemelor eficiente de protecţie împotriva trimiterii mesajelor electronice nesolicitate, reclamantul ar fi putut introduce la instanţele civile o acţiune în daune-interese.

De asemenea în afară de constatările CtEDO, un exemplu vine din Costa Rica, unde Curtea Supremă de Justiție în 2010 a constatat că accesul la internet este drept de bază, prin care se exercită drepturile fundamentale ale democrației.

Concluzii. În contexul celor expuse, după un studiu amplu a jurisprudenței în ceea ce privește încălcările drepturilor omului în Internet, putem reitera următoarele: că Statul are atât obligația negativă de a se abține la orice ingerință în drepturile cetățenilor la libera exprimare pe Internet, cât și obligația pozitivă de a garanta aceste drepturi online, prin implementarea diferitor mecanisme, de exemplu să instituie autorități publice responsabile în domeniul securității drepturilor în mediul online și legiferarea legilor, prin care să se instituie un cadru normativ în domeniu.

În prezentul studiu au fost elucidate aspecte teoretico-practice privind Securitatea Cibernetică prin care se înțelege starea de normalitatea rezultată în urma aplicării unui ansamblu de măsuri practice și reactive prin care se asigură confidențialitatea, integritatea etc.

La examinarea jurisprudenței internaționale în ce privește apărarea drepturilor omului în spațiul cibernetic fiind un domeniu recent dezvoltat, sau analizat cazurile Curții Europene a Drepturilor Omului ce vizează încălcarea drepturilor omului în spațiul virtual, constatând că la momentul actual practica internațională este slab dezvoltată. Însă cu toate acestea, Curtea are deja cazuri unde stabilește că toate drepturile care sunt consfințite în Convenția Europeană pentru Drepturile Omului urmează a fi respectate atât în spațiul real cât și on-line.

Au fost studiate mai multe cazuri ca *Yildirim c. Turciei (Cererea nr. 3111/10)* [1] privind blocarea accesului la toate paginile de internet găzduite de Google pe teritoriul Turciei, Curtea a stabilit încălcarea art.10 din CEDO și a reiterat că acesta se aplică nu doar conținutului informației, ci și mijloacelor de diseminare a acesteia. Curtea a considerat ca efectele ordonanței semnifică "o restricție a accesului la internet", „care a devenit în prezent unul dintre principalele mijloace ale exercitării dreptului la libertatea de exprimare și la informare" [21].

În cazul *Times Newspapers Ltd c.Marea Britanie* (1 și 2) [22], a declarat că: "Cu accesibilitatea lor și capacitatea lor de a reține și de a distribui cantități mari de date, site-uri de pe Internet contribuie în mod semnificativ la îmbunătățirea accesului public la știri și în general pentru a facilita comunicarea

informații. Crearea de arhive Internet reprezintă un aspect cheie al rolului jucat de site-uri , Curtea consideră că se încadrează în domeniul de aplicare al art.10".

Considerăm, că statele sunt obligate să asigure securitatea cibernetică fiecărui utilizator când aceștia sunt *on-line*, pentru ca utilizatorii să-și poată exprima liber opiniile pe Internet, deoarece internetul fiind o modalitate a libertății de exprimare pe internet și a opiniei, se poate realiza doar în cazul când statele se vor angaja la dezvoltarea unor politici eficiente pentru accesul universal la acesta, în caz contrar, Internetul va deveni un instrument care va oferi un decalaj digital și va agrava diviziunile sociale.

Fiind o verigă solidă și totodată cea mai slabă, Securitatea Cibernetică necesită o atenție sporită care necesită de a implementa o cultură strategică comună tuturor statelor lumii și de a elabora și implementa strategii naționale a securității cibernetice comune pentru a putea face față sfidărilor, pentru protecția integrității fizice a cetățenilor, prin sporirea eficienții eficacității și funcționării sigure a infrastructurilor critice și politice de securitate cibernetică, trebuie să ofere un mediu digital sigur și fiabil bazat pe protecția și conservarea libertăților și pe respectarea drepturilor omului on-line, în special protecția vieții private și a datelor cu caracter personal.

Referințe bibliografice:

1. Affaire Ahmet Yildirim c. Turquie, nr.3111/10, 18 decembrie 2012. Hotărîrea din 18 martie 2013. Online: https://hudoc.echr.coe.int/eng?i=001-115401#{%22itemid%22:[%22001-115401%22]}
2. Affaire Leander c. Suediei, nr.9248/81, 26 martie 1987, seria A nr. 116. Online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62077%22]}
3. Ahmet Yildirim c. Turciei, nr. 3111/10, Hotărîrea din 18 decembrie 2012. Online: http://ijc.md/Publicatii/mlu/CEDO/Cauza%20Ahmet%20Y%C3%2584%C2%B1ld%C3%2584%C2%B1r%C3%2584%C2%B1m%20c.%20Turciei_romana.pdf
4. Airey c. Irlandei, Hotărârea din 9 octombrie 1979. on-line: http://jurisprudentacedo.com/Airey-versus-Irlanda-Sot-alcoolic-si-violent-Lipsa-protectiei-Statului.html
5. Alexei Ovchinnikov c. Rusiei, nr. 24061/04, pct. 51, 16 decembrie 2010. Online: www.echr.coe.in
6. August c. Regatului Unit al Marii Britanii. Decizia nr. 36505/02, 21 ianuarie 2003. Online: www.echr.coe.int
7. Copland c. Regatului Unit al Marii Britanii, nr. 62617/00, Hotărîrea din 03 iulie 2007. Online: https://lege5.ro/Gratuit/ge2tqobvg44a/hotararea-privind-cauza-copland-impotriva-marii-britanii
8. Handyside c. Regatului Unit al Marii Britanii și Irlandei de Nord, 7 decembrie 1976, seria A nr. 24. Online: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-62057%22]}
9. K.U. c. Finlandei, nr. 2872/02, Hotărîrea din 02 martie 2009. Online: https://lege5.ro/Gratuit/ge2tqobzgm2q/hotararea-privind-cauza-ku-c-finlandei
10. Kastner Philipp. Cyberjustice in the Context of Transitional Justice, Working Paper n°9, Laboratory of Cyberjustice, November 2013. https://www.cyberjustice.ca/en/publications/cyberjustice-in-the-context-of-transitional-justice/
11. M.C. c. Bulgariei, 04 martie 2004, nr. 39272/98. Online: https://www.coe.int/t/dg2/equality/domesticviolencecampaign/resources/M.C.v.BULGARIA_en.asp
12. Megadat.com SRL c. Moldovei, nr. 21151/04, Hotărîrea din 17 mai 2011. Online: http://agent.gov.md/wp-content/uploads/2015/03/MEGADAT.COM-S.R.L-ART-41-RO.pdf
13. Michael N. Schmitt. Tallin Manual on the international law applicable to cyber warfare. Cambridge University Press 2013.
14. Muscio c. Italiei, (Dosar nr. 31358/03) Decizie CEDO -13.11.2007. Online: https://jurisprudentacedo.com/MUSCIO-c.-Italiei-Receptionarea-in-casuta-postala-electronica-a-

unor-mesaje-nesolicitate-cu-caracter-pornografic-si-ordonanta-de-neincepere-a-urmaririi-penale-ingerinta-inadmisibila.html
15. P.G. şi J.H. c. Regatului Unit al Marii Britanii, 25 septembrie 2001, nr.44787/98. Online: https://jurisprudentacedo.com/PG-si-JH-contra-Marea-Britanie-Supravegherea-persoanei-Conditiile-legii-interne.html
16. Peck c. Regatului Unit al Marii Britanii, 28 ianuarie 2003, nr. 44647/98. Online: https://www.5rb.com/wp-content/uploads/2013/10/Peck-v-UK-ECHR-28-Jan-03.pdf
17. Pravoye Delo și Shtekel c. Ucraina, 33014/05, Hotărâre din 05 mai 2011. Online: hudoc.echr.coe.int/app/conversion/docx/pdf%3Flibrary%3DECHR%26id%3D001-119336%26filename%3DCASE%2520OF%2520EDITORIAL%2520BOARD%2520OF%2520PRAVOYE%2520DELO%2520AND%2520SHTEKEL%2520v.%2520UKRAINE%2520-%2520%255BRomanian%2520Translation%255D%2520summary%2520by%2520the%2520COE%2520Human%2520Rights%2520Trust%2520Fund.pdf%26logEvent%3DFalse+&cd=1&hl=ru&ct=clnk&gl=md
18. Premininy c. Rusiei din 10 februarie 2011, nr. 44973/04. Online: https://www.echr.coe.int/Documents/FS_Detention_conditions_RON.PDF
19. S şi Marper c. Regatului Unit al Marii Britanii [GC] nr.30562/04 şi 30566/04, alin. 103, 4 decembrie 2008. Online: http://www.echr.coe.int/sites/search_eng/pages/search.aspx#{%22fulltext%22:[%22s.%20v%20the%20United%20Kington%22],%22Title%22:[%22s.%20v%20the%20United%20Kington%22]}
20. Sciacca împotriva Italiei, nr.50774/99, alin. 29, CEDO 2005-I. Online:http://jurisprudentacedo.com/Sciacca-contra-Italia-Publicarea-unei-fotografii-Viata-privata-Raport-cu-libertatea-presei.html
21. Site-ul oficial al Curții Europene a Drepturilor Omului. Online: www.echr.coe.int
22. Times Newspapers Ltd c. Marea Britanie, nr.64367/14, Hotărîrea din 13 noiembrie 2018. Online: https://globalfreedomofexpression.columbia.edu/cases/times-newspapers-ltd-v-united-kingdom/
23. X şi Y c. Olandei, 03 aprilie 2012, nr. 42857/05. Online: http://ier.gov.ro/wp-content/uploads/cedo/Cauza-Van-Der-Heijden-impotriva-Tarilor-de-Jos.pdf