Revista Universul Juridic ● nr. 3, martie 2020, pp. 65-136

CULEGEREA DE INFORMAȚII DE SECURITATE NAȚIONALĂ ÎN ERA DIGITALĂ – DIMENSIUNEA ETICĂ

drd. Claudia LASCATEU

Abstract

The study is aiming to convey an interdisciplinary analysis to what gathering intelligence in digital space represents from a legal point of view and what the lack of ethics of such state governed endeavours cause to a democratic society by examining the latest case studies in European and international jurisprudence. To sort out the necessities and scope of intelligence in cyberspace we use the realist, consequentialist and deontological ethical filters in order to realise how developing technologies are connected to the moral compass embedded in human nature.

Keywords: *national security; human rights; rule of law; digital era; private data.*

PRELIMINARII

Realitățile secolului XXI sunt, în esență, guvernate de folosirea tehnologiei pentru a simplifica şi eficientiza traiul uman, numai că aceasta a dus şi la transpunerea funcționalităților comunității în plan digital, întrucât, putem vorbi în prezent de automatizări complexe implicate în serviciul cetățenilor – în unele țări alegerile sunt realizate electronic[1] - gata să identifice cu exactitate orice factori specifici definiți precum un comportament atipic, sau o anumită caracteristică aparte dintr-o multitudine de surse digitale.

Chiar dacă numai prin folosirea unor forme de culegere masivă de date se poate creşte acurateţea rezultatelor, atunci se pune problema reală a ubicuității culegerii de date față de domnia legii, precept fundamental al democrației – „statul trebuie să păzească accesul şi deschiderea, să respecte şi să protejeze drepturile fundamentale ale omului exercitate on-line şi să mențină încrederea în internet şi interoperabilitatea sa" aşa cum prevede Comisia Europeană[2].

---

[1] Australia din 2014, în Belgia din 1991, în Brazilia din 1996, în Estonia din 2007, în Finlanda din 2008, în India din 2011, în Elveția din 2014, în Malaiezia în 2018, în Statele Unite ale Americii din 2000 https://en.wikipedia.org/wiki/Electronic_voting#By_country accesat la 15.01.2020

[2] European Commission *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 2013.

Competiția între lege şi tehnologie este inegală, chiar dacă nevoile societății noastre sunt reflectate în ambele situații, iar legea trebuie să ne protejeze de eventualele încălcări ale drepturilor omului pe care ar putea să le genereze o nevoie de cunoaştere avidă.

În această lucrare, se vor prezenta din perspectivă multidisciplinară cele două ipoteze de cercetare de la care debutează lucrarea, prima parte fiind dedicată analizării dacă etica culegerii de informații din spațiul cibernetic este o expresie a culturii organizaționale şi a doua parte dacă etica culegerii de informații din spațiul cibernetic reprezintă o expresie a aplicării cadrului normativ.

1. CULEGEREA DE INFORMAȚII PERSONALE DIGITALE ÎN INTERES NAȚIONAL

1.1. Natura dreptului la viață privată

Viața privată este un termen care este deseori folosit în jurisprudența în materie de protecția drepturilor omului, care comportă o multitudine de înțelesuri, fiind folosit în plan conceptual ca *umbrelă* ce acoperă o arie largă de drepturi şi interdicții. Pentru unele persoane *viața privată* înseamnă o stare psihologică[3], o extensie a felului în care sunt comunicate informațiile despre ei[4], sau o percep ca starea fizică distinctă, separată de restul societății[5].

Apariția *dreptului la viață privată* în jurisprudență este o susținere a dezvoltării dialectice a dreptului şi a naturii variabile a liberului schimb, asta datorită faptului că dreptul internațional modern diferă de cel practicat în epocile anterioare precum cea a revoluției industriale, a decolonizării, a perioadei de război sau a proiectului democratic care au transformat practicile dreptului internațional. O legătură complexă între tipare comerciale precum Acordul General de Tarife şi Comerț[6], Curtea de Arbitraj Internațional, Medierea disputelor statelor-investitor, Organizația Mondială de Comerț, au apărut, în esență, ca ideologii şi instituții ca reprezentare juridică a realității pe care o trăim.

Istoric vorbind, noțiunea juridică a *dreptului la viață privată* a apărut în practica judiciară din dreptul american la momentul în care camerele de filmat au devenit omniprezente[7], în anii 1950, sub imperiul dreptului civil[8], ca situație în care se

---

[3] Weinstein M.A. *The Uses of Privacy in the Good Life* în Pennock J.R., Chapman J.W., *Privacy: Nomos* ed. XIII Atherton Press, 1971, p. 94.

[4] Westin A.F., *Privacy and Freedom*, ed. Bodley Head, Londra, 1967, p. 7.

[5] Brandeis L.D., Warren S.D, *The Right to Privacy*, The Harvard Law Review vol.4, nr.5, 1980, p. 193-220.

[6] În e*n.* General Agreement on Tariffs and Trade (GATT).

[7] Brandeis L.D., Warren S.D., *The Right to Privacy*. The Harvard Law Review, Vol. 4, nr. 5, 1980, p. 193-220.

[8] În *en.* Tort Law.

impune acordarea unor reparaţii materiale, pecuniare, în situaţia în care acest drept este vătămat şi sunt generate daune morale.

Câteva decenii mai târziu, în anii 1970, al patrulea Amendament[9] a fost interpretat în jurisprudenţa americană ca garant al protecţiei dreptului la viaţa privată în zona de competenţă a dreptului public ca răspuns la apariţia tehnologiei de interceptare[10] folosite de instituţiile de aplicare a legii. În mod simetric, doar în contextul apariţiei internetului, putem vorbi despre apariţia *dreptului de a fi uitat*.

Deci, aşa cum este fundamentat în dreptul european, *dreptul la viaţă privată* este unanim acceptat în sistemele de drept ca *ipostază juridică ce ţine de persoană şi calitatea vieţii sale*. Nevoia de intimitate s-a dezvoltat în răspuns la dezvoltarea socială resimţită tot mai alert în mediul virtual, iar ca expresie juridică, a evoluat odată cu democraţia.

Dreptul de a avea o existenţă protejată intimă, familială şi privată este complex şi este garantat de Constituţia României de la început ca o valoare supremă[11], sporită şi de obligaţia complementară a autorităţilor de stat de a respecta şi proteja indivizii şi viaţa privată[12]. În plus, noul Cod civil român prevede că oricine are dreptul să trăiască, să fie sănătos, să aibă integritate mentală şi fizică, să aibă demnitate, să aibă o imagine de sine, să respecte viaţa sa privată şi aceste drepturi să pot fi transmise[13]. Acestea sunt drepturi fundamentale ale omului, garantate de Constituţia României, care decurg din Declaraţia Internaţionala a Drepturilor Omului. Legea română prevede că oricine are dreptul să aibă un nume şi un loc de reşedinţă legal obţinut. Astfel, aceste atribute nu sunt garantate, deoarece sunt

---

[9] Parte a Constituţiei Americane, al IV-lea Amendament (1789) este o parte a Legii drepturilor garanţii – The Bill of Rights. În acest text sunt interzise percheziţiile şi sechestrul realizate abuziv, impunând regulile minime procedurale pentru obţinerea mandatelor de percheziţie. Totodată, în această secţiune sunt prevăzute sancţiunile pentru încălcarea acestor prevederi. În **1967** Curtea Supremă a Statelor Unite ale Americii a reţinut în cauza *Katz împotriva SUA*, că **prevederile menţionate se aplică şi intruziunilor în viaţa privată a persoanelor, dar şi în imobile**. Pentru majoritatea percheziţiilor şi sechestrelor este necesară deţinerea unei autorizaţii judecătoreşti, cu excepţia percheziţiei consimţite, cele asupra autovehiculelor, a celor în care probele materiale sunt vizibile, cele extraordinare sau la trecerea frontierei. Aşadar, potrivit practicii Curţii, probele obţinute cu încălcarea celui de al IV-lea Amendament sunt inadmisibile în procesele penale.

[10] Cauza ***Olmstead împotriva SUA***, Curtea Supremă de Justiţie a SUA, 04.06.1928, 277US 438. Învinuitul era suspectat de contrafacerea băuturilor alcoolice, aşadar, fără aprobare judecătorească, agenţi federali au instalat mijloace de interceptare în subsolul clădirii în care cel în cauză avea biroul. Acesta a fost învinuit pe baza probelor obţinute din interceptări. Curtea reţine la acel moment că interceptarea conversaţiilor telefonice nu reprezintă o percheziţie sau o sechestrare de bunuri în înţelesul Amendamentului al VI-lea, considerând că aceste prevederi sunt referitoare la acte şi fapte materiale în ceea ce priveşte persoana vizată şi locuinţa sa şi nu acoperă conversaţiile. În final Curtea adaugă că **deşi interceptările reprezintă un comportament neetic, nicio instanţă de judecată nu poate exclude probe doar din considerente morale.** Această practică a fost ulterior inversată în cauza *Katz împotriva SUA 1967.*

[11] Art. 1 din Constituţia României.

[12] Art. 26 din Constituţia României.

[13] Art. 58 NCC al României.

condiționate de urmărirea procedurii legale, dar sunt calități care constituie elementul fundamental al dreptului de a trăi şi de a avea o viață privată

Oricum ar fi definită *viața privată*, există **două concepte ca sunt relevante pentru culegerea de informații**: viața privată ca *limită*, şi viața privată ca *exercițiu al controlului*.

Limitele marchează zonele în care intruziunile externe nu sunt permise, iar acestea ori manifestate fizic ori create ca rezultat al normelor acceptate social, definesc ce este privat, interior, față de tot ceea ce este exterior. Depăşirea acestor limite aşa cum sunt ele marcate înseamnă încălcarea vieții private a acelei persoane. Aceste limite pot fi fizice: pereți, haine, bagaje, sau pot fi metafizice, construcții sociale cum ar fi spațiul intim. Prin comparație, viața privată ca exercițiu al controlului este dreptul indivizilor de a determina acele elemente care îi definesc, respectiv controlul asupra informației despre noi înşine[14] sau controlul asupra chestiunilor personale[15]. Văzută de această manieră, viața privată este strâns legată de dreptul de proprietate în sensul că acțiunile unei persoane şi rezultatele inerente aparțin acelei persoane care le-a generat şi pot fi împărtăşite numai cu aceia cu care acea persoană consideră de cuviință[16].

Atâta timp cât trăim într-o societate unde indivizii sunt în mod unanim intoleranți față de stiluri de viață, obiceiuri, maniere de gândire şi unde defectele umane tind să devină subiect de ridiculizare, dorința generală de a avea viață privată va continua să fie nealterată[17].

De exemplu, şantajul, ca faptă sancționată în dreptul penal, are ca rezultat direct exercitarea puterii de control psihologic şi constrângerea asumării unor costuri materiale dacă anumite fapte ar deveni cunoscute. Asta denotă faptul că viața privată este în sine valoroasă încât faptele legate de constrângerea morală exercitată de expunerea unor aspecte din viața privată sunt ocrotite de legea penală[18]. Deci, indiferent de daunele sociale ori financiare provocate de încălcarea vieții private chiar şi persoanele care afirmă care nu au nimic de ascuns, se opun totuşi ca alți oameni să asculte, sau să vadă ceea ce fac în privat.

Legea română prevede că oricine are dreptul la viața sa privată şi nimeni nu poate fi expus la nicio indiscreție a vieții intime, personale sau familiale, în casa sau corespondența sa, fără consimțământul său sau cu ignorarea restricțiilor şi limitelor

---

[14] Fried C., Privacy, Yale Law Jurnal, art 3, vol. 77, 1968, p. 475.

[15] Gross H., *Privacy and Autonomy* în Pennock and Chapman (eds.) Nomos XIII, Atherton Press, 1971, p. 169.

[16] Shils E., *Privacy: Its Constitution and Vicissitudes*, Law and Contemporary Problems 31/2, Ed. Universității Duke, 1966, pp. 281-306.

[17] Parent W.A., *Privacy, Morality and the Law*, Philosophy and Public Affairs 12/4, 1983, p. 267.

[18] Art. 207 alin. (2) C. pen. – Infracțiuni contra libertății persoanei – **Şantajul** „amenințarea cu darea în vileag a unei fapte reale sau imaginare, **compromițătoare pentru persoana amenințată** ori pentru un membru de familie al acesteia(..)se pedepseşte cu închisoarea de la unu la 5 ani".

impuse de legea națională sau de tratatele pe care România şi le-a asumat[19]. Este, de asemenea, interzisă utilizarea în orice mod a corespondenței, a manuscriselor sau a oricăror alte documente personale, a informațiilor personale fără consimțământul persoanei sau cu nerespectarea reglementărilor[20].

Viața privată, aşa cum este percepută de Curtea Europeană pentru Drepturile Omului prin hotărârea din 2004, în cazul *von Hannover contra Germaniei*[21], este formata din elemente care sunt direct legate de identitatea unei persoane, cum ar fi numele, poza sau imaginea, integritatea fizică şi morală. Garanția prevăzută de art. 8 al Convenției vizează, în principal, asigurarea dezvoltării personalității fiecăruia în raport cu dorința sa, fără o contribuție externă. Datele private nu ar trebui utilizate ca monedă de schimb, ele fac parte din individualitatea fiecărei persoane. Ca şi drepturile de autor, datele personale pot fi folosite, dar nu transferate, proprietarul/utilizatorul are dreptul fundamental de a alege modul în care ar trebui să fie utilizate, deoarece acest tip de date persistă atât timp cât persoana este în viață şi nu poate fi folosite oricând[22].

1.2. Datele private în mediul digital

„Perspectiva divină"[23] oferită de Big Data este izvorâtă din utilizarea de către oameni a tehnologiei digitale, este comportamentală, formată din date granulare care nu sunt legate de identitate care au fost supuse la agregare sau la tehnici incerte în ceea ce priveşte viața privată a utilizatorilor. Aceste informați sunt eminamente digitale, de cele mai multe ori emise ca rezultat al unor activități sau tranzacții şi fără cunoaşterea utilizatorului. Aceste activități includ folosirea comunicațiilor digitale generate de telefonie şi internet.

În ciuda faptului că datele digitale private s-au dovedit a fi o *marfă valoroasă* rezultată din monitorizarea traficului electronic de comunicații destinată generării unor modele de comportament predictiv, pentru a stabili narativele de marketing personalizat (cunoscut ca *micro-targeting*), pentru a determina prin influențare electoratul în timpul campaniilor de alegeri din statele UE şi SUA[24].

---

[19] Art. 75 NCC român.

[20] Art. 71 NCC român.

[21] Curtea Europeana a Drepturilor Omului, *Von Hannover contra Germania*, 2004, https://www.juridice.ro/wp-content/uploads/2016/07/von-Hannover-v-Germany-ECHR-24-June-2004.pdf accesat la 30 octombrie, 2018.

[22] Lascateu C. *The collision between public policy and technology raises the stakes for users*, IKS 2018 Security and Freedom - Contemporary European Policies and Future Perspectives, RISR, no. 19-20/2018, 2019, pp. 433-445.

[23] Pentland. A. *Society s nervous system: building effective government, energy and public health systems,* Pervasive and Mobile Computing, vol. 7, nr. 6, 2011, 643-665.

[24] Lascateu C., *Social media takes a toll on Democracy*, Redefining Community in Intercultural Context, Henri Coandă Air Force Academy Publishing House, 2018, p. 413.

Oricine are dreptul la demnitatea sa, orice atingere a onoarei sau reputației cuiva este interzisă, cu excepția consimțământului dat sau în afara limitelor stabilite de legea română[25]. Dreptul de a avea o reputație este parte din viața privată, aşa cum Curtea Europeană pentru Drepturile Omului a stabilit prin hotărârea sa în cazul *Pfeifer contra Austria* în 2007[26]. Reputația unei persoane face parte din identitatea sa personală şi psihologică şi este subiectul vieții private. Datele personale nu pot fi abandonate, dar utilizatorii au dreptul de a fi uitați de spațiul cibernetic. Nu înseamnă că datele lor vor dispărea, înseamnă doar că motoarele de căutare şi administratorii bazei de date le vor şterge şi nu se vor afişa rezultatele legate de oricare dintre datele private legate de acel utilizator[27].

Ceea ce este interesant este faptul că Regulamentul general privind protecția datelor – (GDPR[28]) se aplică şi statelor care nu sunt membre ale UE şi care prelucrează datele rezidenților europeni, ceea ce înseamnă că modifică şi politica terților părți care sunt interconectați cu bunurile şi serviciile pe piața europeană. Aceasta nu se aplică numai in politica, ci obligă operatorii terță parte să se conformeze, din cauza acoperirii internaționale severe a sancțiunilor impuse de GDPR[29].

1.3. Culegerea de informații prin supravegherea electronică

Ca efect a dezvăluirilor asupra metodelor de culegere a informațiilor în perioada Războiului Rece, s-a pus accent pe creşterea răspunderii consilierilor juridici din serviciile de informații pentru asigurarea legalității operațiunilor în acord cu legislația privind protejarea drepturilor omului, dând astfel naştere unei ***culturi a conformității***[30]. Singura slăbiciune a acestei structuri legale, este că politicile publice ar putea să difere față de acest mecanism procedural care oferă soluții viabile față de normativul din domeniul drepturilor omului.

De aceea, ceea ce se întâmplă în orice organizație cu consilierea juridică, se întâmplă şi în serviciile de informații, respectiv, aportul juridic se limitează la ceea ce au de oferit actele normative pentru situația dată[31].

---

[25] Articolul 72 din Noul Cod Civil Român.

[26] Curtea Europeana a Drepturilor Omului, *Pfeifer contra Austriei*, 2007, https://swarb.co.uk/pfeifer-v-austria-echr-15-nov-2007/ accesat la 30 octombrie, 2018.

[27] Lascateu C. *The collision between public policy and technology raises the stakes for users*, IKS 2018 Security and Freedom - Contemporary European Policies and Future Perspectives, RISR, no. 19-20/2018, 2019, pp. 433-445.

[28] Regulamentul (UE) 2016/679 a fost publicat în Jurnalul Oficial al Uniunii din 4 mai 2016.

[29] Rödl & Partner, *Legea privind confidențialitatea datelor din India şi GDPR al Uniunii Europene*, 24 mai, 2018.

[30] Sprigman C. *The NSA's Culture of "Legal Compliance" Still Breaks the Law*, Just Security, 2014.

[31] Un fost analist şef al NSA afirmă într-un interviu acordat Washington Post că „agenția deține numeroşi juriști iar singurul lor scop este să găsească o modalitate de a respecta legea dar să maximizeze culegerea de informații prin exploatarea fiecărei portițe legislative" (Gellman B., Soltani A. *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say.* Washington Post, 2013).

Această *asigurare a legalității* a fost definită ca **atitudinea etică care ține conduita morală în sfera respectării regulilor şi relații morale constituite din drepturi şi obligații determinate de reguli.** Legalitatea fiind, înainte de toate, perspectiva operațională a profesiei juridice, oriunde te-ai poziționa în proces fiind filonul central împărțit de toți membrii profesiei juridice[32]. După cum spunea şi sociologul Toqueville[33] în secolul XIX „dacă oamenii apreciază libertatea, atunci pun preț şi mai mare pe legalitate. Se tem mai puțin de tiranie decât de puterea arbitrară, şi în condițiile în care legiuitorul se angajează să priveze oamenii de independența lor, ei nu sunt nemulțumiți"[34].

Legalitatea în activitatea de informații aduce *domnia legii* prin consilierii juridici în zona securității naționale şi în culegerea de informații din surse digitale, unde secretizarea îşi modelează impactul într-o serie de modalități foarte importante. Ceea ce este important de observat este că deşi se dovedeşte util, legalitatea în activitatea de informații nu oferă o greutate suficientă libertății personale, întrucât legalitatea produce legitimitatea programelor de restrângere a unor libertăți, iar o atenție desăvârşită acordată drepturilor şi conformării normelor, trece cu vederea ceea ce ar trebui să fie o focusare pe interese, echilibru şi politici publice. Legalitatea în serviciile de informații presupune reguli de bază, control jurisdicțional şi acordarea de competențe consilierilor juridici, toate acestea alcătuind împreună *mentalitatea conformității* activității de informații. Aşadar, axată pe concordanța cu legea şi pe prevalența drepturilor, viziunea despre supraveghere devine acceptabilă şi este chiar încurajată de decidenții politici[35].

O importantă componentă a *legalismului* din activitatea de informații este reprezentată de limbajul juridic folosit, cu terminologia specifică mijloacelor şi metodelor din activitatea de informații, care poate părea că facilitează transformarea regulilor în principii aplicabile măsurilor din acest domeniu, care, în esență, devine mai accesibilă pentru practicieni[36].

Limbajul juridic folosit este foarte important, pentru că este elementul care determină legitimitatea sau lipsa acesteia în situațiile de fapt întâlnite în activitatea de informații. Totodată, prin interpretarea limbajului, a vocabularului folosit în

---

[32] Shklar J. *Legalism: Law, Morals, and Political Trials 1,* Harvard University Press 1964, reed.1986, pp. 12-68.

[33] În cartea *Democrația în America* analizează standardul superior de viață şi nivelul de trai raportat la piețele şi statele din occident.

[34] Tocqueville A. *Democracy in America,* The Pennsylvania State University (1838), reed. 2002 eas3.elte.hu/coursematerial/LojkoMiklos/Alexis-de-Tocqueville-Democracy-in-America.pdf accesat la 02.02.2020.

[35] Schlanger M. *Intelligence Legalism and the National Security Agency s Civil Liberties Gap,* University of Michigan Law School Scholarship Repository, 2015, pg. 117- 185.

[36] Granick J. *The Surveillance State's Legalism Isn't about Morals, It's about Manipulating the Rules,* Just Security, 13.11.2013.

textul normativ, se poate aduce o extindere a aplicabilității normei, față de obiectul inițial avut în vedere de Legiuitor. Interpretarea în sine ca activitate tehnico-juridică este rezervată instituțiilor statului care trebuie să pună norma respectivă în aplicare[37].

De exemplu, **terminologia juridică** folosită de NSA şi GCHQ privind supravegherea în masă este de „acces nelimitat" – *en.* „bulk access"[38] sunt operațiunile de *căutare avansată* a unor itemi preciși într-un vast spațiu de stocare a datelor – în contrast cu terminologia folosită în mediul socio-politic de „supraveghere în masă" – *en.* „mass surveillance"[39] care presupune o *filtrare* constantă a volumelor mari de comunicații din care să rezulte anormalitatea, în speță, un posibil terorist[40].

Diferența subtilă între cele două sintagme poate părea de nuanță, când de fapt relevă tipul de activități realizate, pe de-o parte *bulk access* presupune o disponibilitate constantă şi ubicuă precum şi accesul neîngrădit la date culese prin mijloace cibernetice, sortabile prin soluții de software, pe când *mass surveillance* presupune o filtrare constantă prin aplicații software a volumelor de date culese din mijloace cibernetice, după criterii predefinite(profiluri) şi generarea constantă a unor răspunsuri.

Această diferență naşte şi o interpretare juridică distinctă a situației de fapt, aşadar pe când prima indică existența unei baze de date brute sortabile după anumite criterii, a doua variantă implică existența unei baze de date cu informații deja organizate, integrate. Prima variantă este asemănătoare cu căutarea de informații pe internet printr-un motor de căutare care poate genera rezultate irelevante, însă a doua variantă este similară unei căutări într-o bază de date cu CV-uri, sortate pe profesii.

Deci, accesul *bulk* nu implică în mod obligatoriu accesul la date cu caracter privat, sau la informații confidențiale protejate de lege, dar prin supravegherea în masă, produsul accesat rezultat din procesul de filtrare, este format exclusiv din date şi informații care duc la identificarea persoanei şi a conduitei manifestate

---

[37] Spre exemplu, în dreptul civil, interpretarea legii este realizată exclusiv de Legiuitor sau instanța de judecată.

[38] Termenul a fost folosit de Omand David, fostul director al GCHQ ca o descriere mai exactă a activităților serviciului pe care l-a condus şi a NSA. (Omand D. Sir, *Mass Electronic Surveillance and Liberal Democracy*, Research Centre in International Relations, Department of War studies, King s College London, 21.01.2014).

[39] Terminologie reminiscentă din perioada Stasi a Germaniei de Est, însă, asocierea efectivă cu serviciul de informații respectiv este contestată vehement, datorită formei de guvernământ şi a terorii pe care o instituise asupra populației. În această terminologie, lexical, vorbim de supravegherea maselor, ca formă de control, care poate avea mai multe componente, spre exemplu supravegherea bipolarității politice a populației (în țări a căror formă de guvernământ nu este democratică – Rusia, China, Iran, Turcia).

[40] Fostul ministru de externe al Regatului Unit, William Hague, a sugerat că „dacă nu ai nimic de ascuns nu ai de ce să îți faci griji" (Watts R. William *Hague: British public have 'nothing to fear' from US spies*, The Telegraph, 09.06.2013).

ieşite din comun care a dus la reperarea de către autoritățile îndreptățite să analizeze astfel de informații.

Legislația în materie de supraveghere electronică caută să realizeze un echilibru între securitatea societății şi viață privată a persoanelor, dar programele de supraveghere de generație nouă sunt o reacție la schimbările care au făcut mai dificil de aplicat cadrul legal precis care diferențiază natura juridică a comunicațiilor naționale de cele internaționale.

Explicația rezidă în faptul că urgențele de securitate națională nu permit o amplă perioadă de analiză pentru a personaliza o reacție şi un rezultat care să fie exact încadrat în norma juridică de către Legiuitor, aşa cum se întâmplă în dreptul penal spre exemplu, unde infracțiunea este expres definită în normă, ca faptă urmată de un rezultat periculos şi sancțiunea concretă aplicabilă[41].

Însă, prin aplicarea unor ***standarde în activitatea de informații***, flexibilitatea de acțiune rezultată serveşte scopului de prevenire a materializării pericolului la adresa securității naționale. Nu trebuie pierdut din vedere că partea negativă reprezentată de dirijarea unei forme de activități prin raportare la *standarde* este faptul că rămân zone lipsite de orice formă de reglementare, unde singurul ghid al direcției de acțiune rămâne etica muncii de informații.

Formula *libertate prin securitate* din art. 5 al Convenției Europene a Drepturilor Omului[42], în înțelesul său juridic, nu statuează vreun fel de limitare a accesului serviciilor de informații în viața privată. Dar, în concepția pozitivistă[43], drepturile prin simpla existență reprezintă limita legală recunoscută de lege, unde viața privată nu este doar o chestiune culturală, ci are o valoare juridică determinată[44].

Ca element central, *gândirea morală populară*[45] – ca relativism înrădăcinat atât cultural cât şi juridic – se dovedeşte a fi neadecvată pentru a se adresa noilor provocări nefamiliare din punct de vedere moral şi juridic născute din domeniul

---

[41] Exemplul clasic reprezentat de infracțiunea de furt din art. 228 Cod penal „Luarea unui bun mobil din posesia sau detenția altuia, fără consimțământul acestuia, în scopul de a şi-l însuşi pe nedrept, se pedepseşte cu închisoare de la 6 luni la 3 ani sau cu amendă".

[42] Art. 5 Convenția Europeană a Drepturilor Omului „Orice persoană are dreptul la libertate şi la siguranță"

[43] **Pozitivismul juridic** este un curent de gândire apărut în perioada secolului XVIII – XIX şi reprezintă analiza jurisprudenței pentru formularea unei teorii şi a fost inițiată de J. Bentham şi J. Austin. Opusul acestui curent este *empirismul* care pornea de la fundamentul teoretic pentru care apare jurisprudența.

[44] „Cei care ar renunța la libertatea lor esențială pentru a cumpăra puțină securitate temporară, nu merită nici libertatea, nici securitatea" Benjamin Franklin (Franklin B., Saprks J., Franklin W.T. *The life of Benjamin Franklin: containing the Autobiography, with notes and a continuation,* Whittemore, Niles and Hall, 31.12.1856, p. 244).

[45] Este o ramură a psihologiei care se intersectează cu etica potrivit căruia oamenii de la vârstă fragedă pot lua decizii morale despre ceea ce este bine şi rău, făcând ca **moralitatea să fie o condiție umană fundamentală**. Gândirea morală, este o parte a moralității care apare atât intrinsec cât şi între oameni (Raine A., Yang Y. *Neural foundations of moral reasoning and antisocial behavior*. Social Cognitive and Affective Neuroscience, nr. 1, vol.3, 2006, pp. 203-213).

cibernetic, în care noțiunile de *viață privată* şi *libertate* sunt de cele mai dese ori etaloane universale ce impun respectarea tuturor cetățenilor şi guvernelor. În același timp, aceste deziderate universale raportate la spațiul virtual se îmbină cu pretențiile de a obține anonimitatea şi pretenția de a beneficia de anonimitate, ca drept fundamental.

Potrivit perspectivei filosofice realiste ca rezultat al culturii moralității occidentale în care *conflictele armate implică doar acțiuni imorale*, dacă analizăm actele de decapitare a prizonierilor civili de către Statul Islamic (ISIS/ISIL), se confirmă concepția realistă că *nu există principii morale aplicabile în război*, atunci realismul se dovedeşte a fi validat. Dificultatea rezidă în încercarea de a aplica principiile eticii la dilema reprezentată de conflictele cibernetice, şi mai ales culegerea de informații din acest spațiu[46].

Conceptul de norme emergente este bine stabilit în domeniul juridic sau în ştiințe politice şi relațiile internaționale, dar este văzut cu scepticism în filosofia morală, unde ***normele ca principii morale sunt diferite de practică***[47].

Într-adevăr, încercarea de a deriva norme, precum *bunele practici,* sau încercarea de a concepe norme despre idealuri cum ar trebui să se comporte oamenii sau națiunile, din analiza practicilor actuale, nu poate genera un model logic funcțional datorită faptului că normativul este o parte fundamentală a moralității dar şi a legalității (mai ales în privința relațiilor inter-statale). De aceea, un normativ moral de comportament care să guverneze situații noi, întotdeauna apare din reflexia asupra motivațiilor anterioare pentru a determina comportamentul într-o situație dată. Această concluzie se bazează pe linia de gândire Kantiană, a cărui interpretare a virtuții şi justiției[48], fundamentează viziunile actuale despre rațiunea morală şi autoritatea normelor şi principiilor rezultate. Totuşi filosoful Alasdair MacIntyre[49] este cel care argumentează că ***normativul moral survine din practică şi din învățămintele trase din practică.***

2. CULEGEREA DE INFORMAȚII DIGITALE - PERSPECTIVA REALISTĂ

O încălcare a vieții private este considerată *necesară*, într-o societate democratică, pentru a atinge un obiectiv legitim dacă răspunde unei cereri sociale esențiale şi, mai ales dacă este proporțională cu domeniul legitim prevăzut de autorități

[46] Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare*, Oxford University Press, 2017, p. 40.

[47] Yannakogeorgos P., *The Prospects for Cyber Deterrence: American Sponsorship of Global Norms, Conflict and Cooperation in Cyberspace: The Challenge to National Security,* US Air Force Research Institute, 2013.

[48] Kant I. în lucrarea *The Metaphysics of Ethics*, din 1785

[49] Metodologia sa se bazează pe raționamentul practic, mai ales cum este ghidat de experiență şi judecata matură şi informată, provenită din lucrările aristoteliene despre morală şi filosofie politică. (*Intractable Disputes about the Natural Law: Alasdair MacIntyre and critics,* University of Notre Dame, 2009, pp. 1-52).

pentru a justifica limitarea drepturilor de confidențialitate, motivația este pertinenta şi adecvata a încheiat C.E.D.O. în cauza *Coster contra Regatului Unit* în 2001[50].

Problema care apare pentru culegerea de informații, este totuşi, că unele activități folosite intră în conflict cu una sau mai multe dintre interesele vitale ale persoanei, şi se naşte un motiv întemeiat pentru interzicerea unei astfel de violări. Dată fiind multitudinea de activități subsumate culegerii de informații, ar fi imposibil să identificăm punctual toate ipostazele care pot genera lezări a unor drepturi fundamentale, aşadar, este important să decelăm modalitatea prin care culegerea de informații poate să intre în conflict cu interesele private ale persoanei şi care sunt potențialele daune generate.

Statutul condiționării impuse de etică se referă la acțiunile folosite în culegerea de informații şi ***nu la sursele folosite***.

Viața privată este unul din interesele personale primordiale cu care culegerea de informații intră în conflict, mai ales când mare parte din munca de informații implică demersuri de descoperire a ceea ce oamenii încearcă să păstreze secret. Un bun exemplu este reprezentat de informațiile generate de comunicații. Comunicarea cu alte persoane este o activitate umană prin excelență, fără de care planificarea, organizarea ori desfăşurarea oricărei activități este din ce în ce mai dificilă. Dezvoltarea tehnologiei digitale a exacerbat această componentă şi a fost transpusă în societatea în care trăim, iar pentru serviciile de informații interceptarea acestor comunicații este vitală. Aşa cum spune M. Lowenthal, informațiile din comunicații conferă o imagine asupra discuțiilor, planurilor ori considerațiilor amicilor şi duşmanilor deopotrivă, şi este cea mai apropiată formă de citi gândurile cuiva[51].

Totuşi, prin interceptarea comunicațiilor cuiva i se încalcă intimitatea deoarece întâi activitatea implică interceptarea şi folosirea fără consimțământ a unor informații care în mod esențial sunt proprietatea acelei persoane, şi în al doilea rând, prin violarea unei sfere pe care persoana o consideră privată, reprezentată de distincția clară între interior, acolo unde se realizează comunicarea şi exterior unde se află restul societății. Această distincție interior/exterior este încă aplicabilă, chiar dacă a apărut tehnologia wireless şi comunicațiile din spațiul cibernetic, pentru că şi acest tip de comunicații se rezumă la a fi accesate de persoanele implicate în relaționare, şi nu de publicul larg, deci sunt comunicații private.

2.1 Caracterul nepublic al politicilor de securitate

Se consideră că politicile de securitate națională reprezintă un domeniu excesiv de secretizat, axat pe modul în care sunt exercitate competențele şi justificările legale ale activităților întreprinse în această arie de expertiză, ducând la criticarea

[50] Curtea Europeana a Drepturilor Omului, *Coster contra Regatului Unit al Marii Britanii*, 2001 https://swarb.co.uk/coster-v-the-united-kingdom-echr-18-jan-2001/ accesat la 30 octombrie, 2018.

[51] Lowenthal C., *Intelligence: From Secrets to Policy*, ed. 7, CQ Press, 2017, p .71.

legitimității normelor clasificate. Acest normativ clasificat a fost asociat în lucrările de specialitate cu măsuri deosebite antiteroriste[52] şi programe de supraveghere în masă, criticile formulate fiind axate pe vulnerabilitatea pe care o reprezintă *normele nepublice* față de sistemul democrației în care persistă separația puterilor în stat şi asumarea răspunderii[53].

Însă, *secretizarea din domeniul securității naționale* este considerată de teoreticieni că acoperă de fapt lipsa unei clarități a legii în sine. În unele situații, analiza normativului secret are mai puțin de-a face cu transparența decizională şi mai mult cu eforturile instituțiilor din sistemul de securitate națională de a eficientiza procesul privind formele de control exercitate de puterea legislativă, dar şi de a stabili un cadru de standarde generale adaptabile la un răspuns rapid în situații de urgență. Un argument similar ajută la explicarea fenomenului care se remarcă în normele terțiare potrivit cărora îşi dirijează funcționarea autorităților din sfera securității naționale şi care constă în extragerea principiilor regăsite în normele generale, transformându-le în standarde[54].

Totuşi, din punctul de vedere al secretizării specificului activității de informații, şi, în mod conex, secretizarea standardelor de dirijare a specificului muncii, se pot estompa tensiunile ce ar putea apărea față de imposibilitatea de punere în aplicare a unei măsuri datorită limbajului juridic folosit în norma de bază, generală.

Dezvoltarea unor mijloace de reglementare interne prin standardizare, acel fenomen denumit *drept flexibil*[55] despre care vorbeam ca fiind un proces organizațional determinant, care căpătă conținut juridic şi produce rezultatele scontate în anumite situații predefinite, şi care depăşeşte analiza logico-juridică punctuală,

---

[52] Precum operațiunile secrete de capturare şi exfiltrare a suspecților de terorism realizate de CIA (en. *extraordinary rendition*) sau atacurile cu rachete de la distanță realizate de armata SUA prin folosirea dronelor.

[53] Concluzia autorului este că există protecție *într-un grad limitat* în Constituție în fața unei secretizări abuzive, şi că există o incompatibilitate între secretizare şi separația puterilor în stat şi asumarea răspunderii în mod democratic (Stone G. R. *Secrecy and Self-Governance,* 56 New York Law School Law Review 81, 2011).

[54] Un exemplu este ***Legea*** privind protecția informațiilor clasificate nr. 182/2002, cu norma de aplicare ***Standardele naționale*** *de protecție a informațiilor clasificate în România*, aprobate prin Hotărârea de Guvern nr. 585/2002. În mod similar, normele terțiare, de punere în aplicare a cadrului de bază, care datorită specificului activității instituției în ecosistemul de securitate națională, pot avea caracter clasificat, deci nepublic, cu valoare de standard pentru linia de muncă reglementată.

[55] en. *soft law*, fr. *droit mou,* este reprezentat de un ansamblu de reguli a căror formă este flexibilă, asemenea normelor de etică a unei profesii, dar care comportă o specificitate crescută datorită organizației în care se aplică şi culturii organizaționale. Aceste reguli nu pot fi sancționate ca o într-o ramură de drept prin aplicarea legii, ci evoluează şi sunt adaptate odată cu personalul din organizație şi influențele externe ce apar, dar nu au forța juridică a legii. Este o formă de drept împrumutată din dreptul internațional – en. *soft law* – ca derivat din dreptul cutumiar. (European Center for Constitutional and Human Rights https://www.ecchr.eu/en/glossary/hard-law-soft-law/ accesat la 18.02.2020).

privită din exterior poate duce la concluzia eronată că lipsa de claritate a legii generale se confundată cu normativul clasificat al unui serviciu de informații.

Totuşi, trebuie remarcat că domeniul securității naționale a depăşit epoca excepționalismului juridic, problemele care se pun fiind din sfera respectării drepturilor fundamentale ale omului[56] şi a transparenței instituționale ca factor de asumare politică.

Scopul principal al *domniei legii* (a statului de drept) este să asigure respectarea regulilor şi evitarea arbitrariului, pentru că asta înseamnă supremația absolută şi predominanța legii ordinare, în contrast cu influențele puterii arbitrare, şi exclude existența arbitrariului, şi a acestor prerogative din sfera guvernământului[57].

Sub aspectul *moralității legii*, această analiză introspectivă este rezervată doar destinatarilor respectivului normativ, care se bucură de încrederea conferită de reprezentanții societății pentru a acționa în cea mai justă şi legitimă manieră pentru îndeplinirea misiunii încredințate, fie ea şi nepublică.

Chiar dacă ar părea a fi pusă în umbră această latură a dreptului flexibil, datorită nevoii de a fi păstrat secret, şi, inerent în această ipostază, datorită imposibilități determinării a obligativității respectării legii datorită neîndeplinirii condiției de opozabilitate *erga omnes.* „Nu poate exista un motiv rațional pentru care să afirmi că o persoană are obligația morală de a respecta legea care este păstrată secret față de ea”[58]. Aceasta este o construcție logică care pleacă de la ipoteza că *secretizarea poate ascunde abuzuri*, când încă din principiile aplicării clasificării unor activități sau mijloace, elementul protejat prin secretizare este securitatea națională, binele general al societății şi păstrarea formei de guvernământ democratic a statului. În Legea română este interzisă alocarea unui nivel de secretizare informațiilor de interes public sau a acelor date care ascund săvârşirea unei infracțiuni[59].

De asemenea, secretizarea poate reprezenta o deviație de la *principiul legalității* pentru că pe de-o parte ascunde autoritatea legală prin care se exercită puterea de stat, dar şi prin faptul că ascunde mijloacele şi metodele prin care exercită puterea de stat acea autoritate. Deci, pe această linie logică secretizarea ar putea submina şi

---

[56] Hafetz J. *A Problem of Standards? Another Perspective on Secret Law,* William & Mary Law Review, vol. 57, 2016, pp. 4-5.

[57] Dicey A.V. *Introduction to the study of the law of the constitution,* Library of Congress Cataloging in Publication Data, ed. 8, Macmillan, Londra, 1915 reed. http://files.libertyfund.org/files/1714/0125_Bk.pdf accesat la 04.02.2020.

[58] Filosof al dreptului, autorul argumentează că toate sistemele de drept conțin o „moralitate intrinsecă” care impune persoanelor o obligație prezumtivă de a o respecta. (Fuller L.L. *The morality of Law,* ed.2, Yale University Press 1969, pp.33-94).

[59] Art. 24 alin.(4) din Legea nr. 182/2002 *privind protecția informațiilor clasificate* „Se interzice clasificarea ca secrete de stat a informațiilor, datelor sau documentelor în scopul ascunderii încălcărilor legii, erorilor administrative, limitării accesului la informațiile de interes public, restrângerii ilegale a exercițiului unor drepturi ale vreunei persoane sau lezării altor interese legitime”.

principiul egalității în fața legii, acordând autorității respective abilitatea de a trata subiecții de drept diferit, ducând la o practică neunitară, discriminatorie[60].

Această linie de gândire pleacă de la ipoteza că orice persoană este subiect de drept de competența unui serviciu de informații, şi doar unele persoane fac obiectul măsurilor specifice de culegere de informații, care au un regim clasificat, fapt care naşte un tratament discriminatoriu. Totuşi în combaterea acestei linii de argumentare, şi mijloacele de atragere a răspunderii din cadrul dreptului penal comportă o parte investigativă în cadrul urmăririi penale care nu se aduc la cunoştința învinuitului decât în momentul punerii sub acuzare. Mai mult, în Legea națională română este statuat că nu se atribuie o clasă de secretizare informațiilor în scopul ignorării Declarației Universale a Drepturilor Omului[61].

Deopotrivă, secretizarea este văzută ca reprezentând o amenințare la *asumarea răspunderii şi separația puterilor în stat*, deoarece atât activitatea desfăşurată de stat cât şi raționamentul juridic pe care s-a fundamentat respectiva activitate rămâne ascunsă față de public, cheile de control democratic obişnuite într-o societate democratică nu mai pot funcționa[62].

Chiar dacă activitatea secretizată nu este supusă evaluării publice, transparente, ca orice activitate desfăşurată de instituțiile publice, totuşi activitatea de informații ca secret de stat[63] este supusă controlului exercitat de parlament, sau de justiție în condițiile în care în România atât parlamentarii, cât şi magistrații au acces de drept la informații clasificate[64].

---

[60] Autorul explică modalitatea prin care principiul legalității în drept impune tratamentul egal al persoanelor, şi este realizat numai atunci când statul practică regularitatea, publicitatea şi generalitatea. (Gowder P. *The Rule of Law and Equality,* Law and Philosophy, vol.32, nr. 5, Springer, 2013, pp. 565-566)

[61] Art. 3 din Legea nr. 182/2002 *privind protecția informațiilor clasificate* „Nici o prevedere a prezentei legi nu va putea fi interpretată in sensul limitării accesului la informațiile de interes public sau al ignorarii Constituției, a Declarației Universale a Drepturilor Omului, a pactelor şi a celorlalte tratate la care România este parte, referitoare la dreptul de a primi şi răspândi informații".

[62] Kutz C. *Secret Law and the Value of Publicity,* Ratio Juris vol.22, nr.2, 2009, pp. 197, 201.

[63] Art. 10 din Legea nr. 51/1991 *privind securitatea națională*, republicată „Activitatea de informații pentru realizarea siguranței naționale are caracter secret de stat".

[64] Art. 7 alin. (4) lit. d)-g) din Legea nr. 182/2002 *privind protecția informațiilor clasificate* „Accesul la informații clasificate ce constituie secret de stat, respectiv secret de serviciu (...) **este garantat, sub condiția validării alegerii sau numirii şi a depunerii jurământului**, pentru următoarele categorii de persoane: **deputați, senatori, judecători, procurori;**

2.2. Factorii determinanți pentru culegerea datelor private digitale prin supraveghere

Pornind de la conceptul de *panoptic*[65] al lui J. Bentham[66] din secolul XVIII şi cel integrat în criminologie[67] de M. Foucault[68] referitor la culegerea de informații din spațiul public, prin mijloace tehnice, în scopul prevenirii săvârşirii faptelor de natură penală, ajungând la supravegherea realizată de serviciile de informații pentru protejarea societății în care trăim, competențele de supraveghere ale statului sau ale corporațiilor sunt considerate, ori o încălcare inexplicabilă a democrației, ori o necesară expresie a progresului fenomenului tehnologic şi a securității. Însă, principiile morale reprezentate de proporționalitate, legalitate şi necesitate, au devenit standardele actuale ce trebuie aplicate erei digitale.

---

[65] Termenul **panoptic** provine din grecescul *panoptes* – atotvăzător. Un tip de clădire a unei închisori şi, totodată, un concept de sistem de control inventat în secolul XVIII care presupune ca un singur gardian să supravegheze toți deținuții. Deşi fizic nu este posibil ca un singur gardian să vizioneze toate celulele în acelaşi timp, faptul că deținuții nu pot cunoaşte momentul în care sunt supravegheați îi va motiva să se comporte corespunzător din proprie inițiativă. Arhitectura respectivă presupune o clădire circulară. (V. Cioclei *Manual de criminologie* C.H. Beck, 2019, pp. 9-15)

[66] **Jeremy Bentham –** filosof şi jurist britanic, reformist social al secolului XVIII, este părintele a curentului utilitarist. Definit de axioma fundamentală a filisofiei sale este principiul că „cea mai mare fericire a celor mai mulți, aceea este măsura Binelui şi a Răului". A fost cel care a ghidat filosofia dreptului Anglo-American şi a radicalismului politic ale cărui idei dus la fondarea unui tip de curent consecințialist denumit *welfarism* ce constă în faptul că acțiunile, politicile şi/sau regulile ar trebui evaluate pe baza consecințelor lor. (Burns, J. H. Happiness and Utility: Jeremy Bentham's Equation, Utilitas. 2005, pp. 46–61) **Welfarismul** este curentul filosofic prin care consecințele semnificate în plan moral sunt de fapt acțiuni directe asupra bunăstării umane sau a vieţuitoarelor. Acest curent are în principal în vedere bunăstarea economică şi a reprezentat o influență în legiferare şi în mişcările sociale.

[67] Termenul provine din latină – *crimen* - acuzație, derivat din greaca antică *krino* şi *logos* însemnând *cuvânt* şi *motiv* sau *plan*. Conceptul a apărut în secolul XIX (profesorul de drept italian **Raffaele Garafalo**) ca ştiință interdisciplinară cu scopul de a studia natura, întinderea, managementul, cauzele, controlul, consecințele şi prevenția comportamentului criminal, atât la nivel individual, cât şi social. (Cioclei V. *Manual de criminologie* C.H. Beck, 2019, pg.11-20.)

[68] **Michel Foucault -** filosof francez al secolului XX, ideolog şi teoretician al ştiințelor sociale a lansat teoria potrivit căreia **legătura între putere şi cunoaştere este folosită ca o formă de control social prin instituțiile statale**. Acesta a argumentat că societățile vestice contemporane au evoluat la *societăți disciplinare*, *societăți ale controlului.*(Deleuze G. *Postcript on the Societies of Control,* The MIT Press, vol.59, 1992, pp. 3-7). **Contribuția sa la criminologie este că esența controlului infracțiunilor s-a schimbat de la amenințarea cu pedeapsa respectiv teama de a fi pedepsit fizic, la controlul prin supraveghere – teama de a fi văzut făcând ceva greşit, ilegal**. Pedeapsa s-a schimbat de la un spectacol public a unor violențe fizice, la a fi aplicate în spetele uşilor închise, de la a fi rapidă şi aplicată corporal, la a fi de durată şi psihologică – pedepsele în prezent au scopul de schimba mentalitatea. Asta reflectă **felul în care puterea este exercitată în societate**. În viziunea sa **supravegherea este văzută ca putere disciplinară şi se extinde în întreaga societate**.(Thompson K. *Foucault – Surveillance and Control,* Crime and deviance, Revise Sociology 2016)

Unde lumea lui Hobbes[69] este delimitată de teritorialitate, lumea modernă a serviciilor de informații este globală şi transnațională, iar distincția dintre cetățean şi străin se remarcă la orice trecere de frontieră. Totuşi, există o disipare a limitelor în spațiul cibernetic, pe acest teren nelimitat al posibilităților unde apare inerent comunitatea de servicii de informații SIGINT, care formează un sistem care, aşa cum spunea Foucault, nu funcționează pe modelul represiv, ci doar în condițiile impuse de productivitate, şi de drepturile şi libertățile personale. Deci, într-o perspectivă democratică, orice practică represivă reprezintă un act de regres. Acest exemplu arată că securitatea se obține prin libertate, şi nu se realizează *securitatea cu costul libertății*. Aşa a ajuns ca spațiul digital să reprezinte *manifestarea tehnologică a unei libertăți transformate în care se pot realiza formele de comunicare* precum discursul politic, socio-cultural, pedagogic şi economic. Dilema în care se află factorii politici este găsirea unei maniere de reglementare a acestei zone de comunicare nestingherită, ce tehnologii de control pot fi antamate care la rândul lor nu pot fi limitate de teritoriu sau autoritatea suverană a statului, precum şi dacă astfel de tehnologii pot fi create, definite exclusiv digital, produse software şi nu hardware, anonime dar totuşi transnaționale şi globale ca întindere a efectelor[70].

Dacă luăm în calcul conceptul de *capitalism al supravegherii*[71] ca expresie a culegerii de informații din spațiul public conexat cu interesele politico-economice din spatele creşterii acestui fenomen, aceasta ar putea oferi o explicație necesară nevoii avide de date din sectorul industrial. În urma identificării raporturilor juridice ce se nasc în cazul supravegherii *în masă*, şi a actorilor ce beneficiază din dezvoltarea sa, apare ca imperios necesară calificarea limitărilor dreptului la viață privată precum şi regimul juridic aplicabil. Totuşi, analizând componentele economiei moderne se observă cu claritate faptul că acestea încurajează dezvoltarea tehnologiilor sofisticate de supraveghere, iar în acest context, internetul a devenit un instrument optim de supraveghere, împotriva căruia se străduieşte să prevaleze dreptul la viață privată[72].

Din această paradigmă, s-a născut şi conceptul de „intimitate de grup" – *group privacy* – în care, datorită analizei big data individul privat se pierde în categorii de

---

[69] Thomas Hobbes, filosof britanic din secolul XV considerat fondatorul filosofiei politice moderne, cunoscut pentru opera Leviatanul în care se naşte **teoria contractului social.** Doctrina sa stă la baza formării statului şi guvernării legitime, **bazate pe moralitate** (Lloyd S.A., Sreedhar S. *Hobbes s Moral and Political Phiosophy,* Stanford Encyclopedia of Philosophy, 12.02.2012).

[70] Bauman Z., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. *After Snoeden: Rethinking the Impact of Surveillance,* International Political Sociology, nr.8, 2014, pp.18-19.

[71] Termenul a fost introdus în **2015** de R. McChesney şi J.B. Foster în publicația Monthly Review. În acelaşi an S. Zuboff a folosit termenul pentru a descrie *logica acumulării* din spatele modelelor de business reprezentate de giganții internetului Google şi Facebook. (Zuboff S. *Big other: surveillance capitalism and the prospects of an information civilization*. Journal of Information Technology 2015, pp. 75-89)

[72] Latimer J. *A Commodity-Form Critique of Mass Surveillance, School of Governance, Law and Society, Tallinn University, 2017,* pp. 10-15.

grupuri de oameni generate de anumite elemente ale vieții sale, precum predilecția pentru un anumit site de cumpărături şi nu mai depinde de elementul cultural, ca în teoria clasică. Deci analiza big data naşte clasificări sociale bazate pe profiluri aplicate la o scară care depăşeşte granițele teritoriale. Faptul că persoana în sine nu mai este centru, ci doar incidentă unui grup, ca parte a unui proces, pune la încercare chiar fundamentul juridic existent, standardele etice şi teoriile clasice. Posibilitățile tehnologice şi costurile financiare implicate în culegerea de informații şi procesarea acestora au fost un factor de limitare a întinderii datelor ce pot fi stocate, procesate şi utilizate, de aceea a fost nevoie de stabilirea unor criterii de selecție a datelor ce trebuie stocate, despre care persoană, obiect sau proces şi pentru cât timp. În consecință, procesarea datelor afecta des doar anumite persoane sau grupurile mici, de aceea, normele legale şi standardele etice s-au dezvoltat în jurul persoanei în particularitatea sa. Dar, odată cu diminuarea costurilor de culegere, stocare şi analiză a volumelor masive de date, se observă şi o schimbare calitativă care modifică în esență bazele teoriilor sociale, juridice şi etice, precum şi ale practicii care s-au dezvoltat în ultimele decenii[73], întrucât spațiul cibernetic nu este doar o proiecție a individului, a societății şi a principiilor organizării statale în care trăim, este proiecția tuturor indivizilor, a societăților culturale, şi a statelor, simultan şi perpetuu.

Deşi în teorie există o diferență între mecanismele de drept privat privind protecția datelor cu caracter personal culese de agenți economici şi remedii ce țin de drept public (control parlamentar sau judecătoresc) împotriva intruziunilor în viața privată, acestea converg în aceeaşi direcție[74], arătând, de fapt, interdependența dintre programele de supraveghere guvernamentale şi supravegherea de masă realizată în scop comercial.

Supravegherea este un exemplu prin care interesele personale sunt afectate de culegerea de informații, atât viața privată cât şi autonomia persoanei printr-o multitudine de activități precum camerele CCTV, filajul[75], traficul de date online[76] sau examinarea unui volum mare de informații din baze de date pentru a genera informații noi *(data-mining[77])* pentru a stabili cine este acea persoană, unde se

[73] Taylor L., Floridi L., van der Sloot B. *Group Privacy: new challenges of data technologies,* Springer, 2017, p. 12-63.

[74] Moglen E. *Snowden and the Future: Part IV; Freedom's Future*, 2013, p. 5, 9.

[75] Northcott C., *The Role, Organisation and Methods of MI5*, International Journal of Intelligence and Counterintelligence nr. 20/3, 2007, pp. 453-79.

[76] Atunci când o persoană este supravegheată prin monitorizarea amprentei digitale, colectare de date care generează un **profil** care ajută la predicția unui mod de acțiune sau localizarea unei persoane.

[77] Este procesul prin care se dezvoltă tipare în seturi mari de date şi implică metode complexe, aflate la intersecția dintre machine-learning, statistică şi sisteme de baze de date. ***Data mining*** este un subdomeniu interdisciplinar al informaticii şi statisticii cu un scop global de a extrage informații prin mijloace inteligente dintr-un set de date, şi să transforme informația într-o structură inteligibilă şi utilizabilă.

îndreaptă, cu cine se asociază sau ce demersuri întreprinde. Pe lângă faptul că acest tip de informații rezultă din dreptul fundamental de proprietate al persoanei, se încalcă şi libertatea de acțiune, alt drept fundamental al omului.

Controlul asupra vieții private a unei părți din societate[78] reprezintă un stimulent puternic pentru guvernanți, în prezent materializat prin controlul digital exercitat asupra fluxului de date vehiculate pe internet în state a căror formă de guvernământ este autoritară precum China, Turcia, Iran, Rusia, Coreea de Nord, aceste state fiind susținătorii teoriei *teritorialismului spațiului virtual* pentru desăvârşirea controlului asupra informațiilor vehiculate de populație[79].

Deci, în acest caz, un indiciu al *abuzului de putere* este reprezentat de prerogativa de a avea acces la informații protejate sau sensibile fără a justifica necesitatea sau scopul demersului în fața populației. A existat o perioadă de expansiune a culegerii de date, dar acest fapt nu este caracteristic doar agențiilor guvernamentale a statelor-națiune menționate, în ultimii 10 ani, agenții economici transnaționali au dat o valoare pecuniară datelor private culese de la clienții lor[80].

Ceea ce este important în supravegherea în masă este *dimensiunea transnațională*, deci problema aplicării extrateritoriale a prevederilor privind drepturile omului prezintă o mare importanță din perspectiva jurisdicțională.

De la apariția dezvăluirilor lui Eduard Snowden[81], au fost aduse în prim plan discuțiile privind inadecvarea cadrului legal privind de protejarea vieții private în mediul cibernetic.

În contextul dezvăluirilor publicul larg a fost pus în fața problemei ridicate de supravegherea realizată de serviciile de informații când s-a aflat că Agenția Națională de Securitate americană (NSA) a cules informații despre proprii cetățeni şi alți actori statali[82] prin toate mijloacele tehnologice disponibile, apărând astfel

---

[78] Partea din societate care activează în spațiul cibernetic.

[79] Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019, p .56.

[80] Charluet C. *It's possible to monetize data while respecting consumer privacy – here's how*, Growth, 2019.

[81] Fost angajat al Agenției Centrale de Informații (CIA), ulterior al subcontractorilor acestui serviciu de informații s-a hotărât să divulge publicului, în 2013, prin intermediul BBC News mijloacele şi dimensiunea supravegherii realizate de angajatorii săi, generând o serie de întrebări asupra moralității mijloacelor de recrutare folosite în munca de informații de angajatorului său. Pe situl the Biography Channel, a publicat informații adunate de-a lungul anilor, iar în mai 2013 a predat unui jurnalist The Guardian informații despre guvernul Statelor Unite ale Americii. Ainuvee Kr, *The Impact of Snowden's Revelations on the Perception* of the US, 26.11.2013. Edward Snowden este acuzat de trădare în SUA şi a obținut azil în Rusia datorită dezvăluirilor sale despre programele secrete de supraveghere ***Xkeyscore, Upstream, Quantuminsert, Bullrun*** şi ***Dishfire.*** precum şi ***Tempora*** cu aplicațiile ***Optic Nerve.***

[82] Germania şi Brazilia au avut reacțiile cele mai vocale. (Lynch C., Harris S., Hudson J. *Germany, Brazil Turn to U.N. to Restrain American Spies*, 14.10.2013, Foreign Policy), http://www.foreignpolicy.com/posts/2013/10/24/exclusive_germany_brazil_turn_to_un_to_restrain_american_spies accesat la 16.01.2020.

dileme asupra însemnătății suveranității şi legitimității politice față de ***normele democrației în era digitală***.

Un caz adus în fața Curții Supreme a Regatului Unit este, în esență, reprezentat de cauza *Catt*[83] dovedirea culegerii de informații din supraveghere electronică în spații publice şi crearea unui profil de interes pentru instituțiile statului prin multiple cereri de acces la informații de interes public realizate de un activist de 90 de ani care participa la proteste împotriva industriei de armament. Decizia Curții Europene a Drepturilor Omului (CEDO) atestă faptul că datele reclamantului au fost reținute în ciuda faptului că *nu* reprezenta o amenințare la securitatea națională, chiar dacă jurisprudența anterioară arăta că o culegere de informații din toate sursele de informații disponibile în scopul prevenirii criminalității şi păstrării ordinii publice este legală şi urmăreşte un scop legitim. În cazul de față datele şi informațiile stocate de autorități s-au considerat a fi disproporționate şi fără a dovedi o necesitate, Curtea subliniind că practica judiciară britanică nu a relevat natura sensibilă a unor date reținute despre Carr, mai ales cele privind opiniile politice şi apartenența la sindicat, atrăgând atenția asupra ambiguității identificate în politica legislativă britanică privind bazele de date deținute şi lipsa mijloacelor de prevenire a arbitrariului şi a abuzurilor.

Concluzia care se relevă este că **există subiectivism în aplicarea normelor legale** fapt ce se observă chiar din jurisprudență, iar datele cu caracter personal capătă o valoare patrimonială, asta rezultând distinct din evaluarea daunelor morale în procesele în care s-a stabilit ingerința asupra vieții private.

2.3. Elementele realismului în culegerea de informații private digitale

Tabloul juridic actual privind exercițiul puterii guvernamentale în domeniul securității naționale, de la folosirea forței militare, la culegerea masivă de date, arată o imperfectă, câteodată chiar o stufoasă combinație de reguli şi standarde. Aşadar, secretizarea rămâne o temă importantă în baza căreia se pot estompa discrepanțele din substratul juridic pe care se fundamentează autoritatea măsurilor întreprinse de autoritățile din sfera securității naționale.

---

[83] Cauza *Catt* împotriva *Regatului Unit* (Curtea Supremă a Regatului Unit 2015 şi decizia finală a CEDO **2019**) are ca obiect faptul că dl Catt a început în 2005 să participe la protestele unei ONG cunoscută pentru proteste violente, unde prezența Poliției era substanțială. În 2010 a cerut poliției comunicarea datelor deținute despre dumnealui la care a primit 66 de nominalizări din dosarele altor persoane şi rapoarte în care era menționat despre incidente din perioada 2005-2009, dar şi alte 13 informații care nu aveau legătură cu protestele, date extrase din baza de date a Poliției denumite „baza de date cu extremism". În 2010 reclamantul a cerut ştergerea datelor şi informațiilor din evidențele Poliției, cerere încuviințată în 2012 iar în bazele de date au rămas doar 6 rapoarte. Curtea Supremă a reținut că reținerea datelor respective a fost realizată cu încălcarea dreptului la viață privată, dar stocarea acelor date nu a produs o pagubă reclamantului, întrucât s-a dovedit necesară. În 2019 Curtea de la Strasbourg a dat câştig de cauză reclamantului, dreptul său la viață privată a fost încălcat, acordând daune morale reclamantului.

În consecință, apar două strategii ce se extrag din prisma realismului[84] pentru adresarea *rolului constructiv al considerațiilor morale în abordarea culegerii de informații din spațiul cibernetic*: prima implică explorarea avantajelor reprezentate de moralitate ca formă de autodeterminare[85] în contrast cu constrângerile externe şi arbitrare impuse de lege[86], pe când a doua se poate considera pe de-o parte ca rezultat a primei, dar care presupune ca persoanele să se intereseze mai mult de ceea ce reprezintă etica în cadrul organizării sociale[87], şi cum aceasta poate în mod plauzibil să confere un ghid universal pentru comportamentul uman şi exercitarea superiorității morale[88].

Ambele variante sunt importante în justificarea eficienței aplicării principiilor eticii realiste în activitățile desfăşurate în spațiul virtual.

Într-adevăr, cele două perspective au un caracter subiectiv dar şi psihologic privind atitudinea celor guvernați față de constrângeri autoimpuse care rezultă din urmărirea satisfacerii intereselor naturale, sau din concepția acestora asupra

---

[84] În Grecia Antică, în secolul IV î.Hr, Tucidide (istoric şi general) este considerat inițiatorul **realismului politic –** curent prin care comportamentul politic şi rezultatele relațiilor inter-statale sunt influențate şi construite pe sentimentul de *teamă* şi pe *interesele personale al oamenilor* (Harloe K., Neville M. *Thucydides and the Modern World: Reception, Reinterpretation and Influence from Renaissance to the Present*, Cambridge University Press, 2012, p. 12). Din ideea expusă de Tucidide potrivit căreia natura umană explică comportamentul oamenilor în situații de criză, de război, a apărut **teoria stimulentului** propusă de J.N. Moore din îmbinarea teoriilor idealiste şi realiste. Această teorie explică apariția conflictelor armate, plecând de la modelul păcii democratice kantiene şi de la principiul descurajării conflictului armat (Moore J.N. *Solving the War Puzzle: Beyond the Democratic Peace,* Carolina Academic Press, 2017).

[85] **Principiul autodeterminării** stă la baza dreptului internațional modern, ce se regăseşte în capitolul I din Carta Națiunilor Unite. Carta statuează că în baza respectării egalității în drepturi şi a tratamentului, oamenii au dreptul să îşi aleagă singuri suveranitatea şi statutul politic în plan internațional. Acesta principiu este derivat din **principiul etic kantian** potrivit căruia **omul are autonomia de a decide aplicarea unui principiu moral.**

[86] Adepții realismului consideră că actorii principali în spațiul internațional sunt **statele** care se preocupă în principal de propria securitate, acționează în scopul propriilor interese naționale, şi se luptă pentru putere, fiind **sceptici față de relevanța principiilor etice** în relaționarea cu celelalte state.

[87] Ideea se naşte din teoria etică a responsabilității sociale a organizațiilor, care este legată în mod direct de cultura organizației. Chiar dacă este într-o strânsă legătură cu comportamentul organizațional şi psihologia mediului organizațional respectiv. **Etica organizațională** exprimă valorile acelei organizații către membrii săi dar şi către alte entități conexe, indiferent de cadrul legal existent. Scopul unei organizații etice este ***binele tuturor***. Se pune preț pe relațiile interne dintre lideri şi angajați, dar şi relațiile externe cu celelalte entități şi cu comunitatea. Ca rezultat imediat **relațiile interumane se îmbunătățesc** şi se naşte ***o cultură a eticii***. (Brimmer S.E. *The Role of Ethics in 21st Century Organizations* Leadership Advance online, nr. XI, 2007).

[88] Realiştii consideră absența unei forme de guvernământ ca fiind anarhie, iar relațiile internaționale, în viziunea acestora sunt predominate de o stare anarhică care generează schimbările din această sferă. Totodată, în optica realistă **securitatea** joacă un rol central, explicând că acesta **este determinată de putere**, de aceea statele încearcă constant să câştige putere pentru a descuraja adversarii potențiali. Această viziune rezultă din concepțiile filosofului din secolul XVI, T. Hobbes, ce pune bazele neorealismului.

noțiunii de Bine, în sensul dirijării acțiunilor lor pentru *obținerea binelui*, conform perspectivei kantiene.

Astfel de principii autoimpuse care guvernează activitățile umane par că au o şansă mai bună de a câştiga respectul general, aprobarea şi conformarea în societate, mai ales când este confruntată cu constrângerile ce par arbitrariu impuse prin lege. La fel cum *buna guvernare* şi *domnia legii* sunt au gradul cel mai ridicat de eficiență când survin din necesitatea consimțită a celor guvernați de a impune ordine într-o stare de anarhie, spre beneficiul tuturor[89].

Necesitatea de organizare, de stabilitate, este o proiecție a umanității de a încadra într-o zonă formală a viziunii comune asupra principiilor morale unanim acceptate, care ar trebui să guverneze acest spațiu nou, virtual. Aceasta este una din explicațiile social culturale pentru interesul de a dezvolta o formă de a accesa conştiința celor care desfăşoară activități în mediul cibernetic, care are un caracter transnațional. Principiile morale sunt independente de paradigme legate de cultură şi spațiu național şi funcționează în situații în care procedurile din normele legale par imposibil de aplicat, pentru a restabili ordinea şi a rezolva conflictele într-o varietate de spații de exercitare a formelor politice de organizare a societății.

Aşadar, în timp ce principiile morale şi cerințele eticii au dezavantajul de a părea ambigue şi deschise către o varietate de interpretări, acestea se dovedesc potrivite pentru a reda ordinea şi a proteja drepturile fundamentale trecând peste delimitările culturale şi politice, față de întinderea jurisdicțională a legii, ori cea cutumiară a relațiilor internaționale.

Chiar dacă înțelegerile cu caracter normativ dintre state au, de regulă, ca fundament principii morale, acestea se pot altera, aşa cum arată istoria dreptului internațional umanitar şi a drepturilor omului, iar aceste principii pot fi proiectate în spațiul cibernetic, în care dispar logicile survenite din cutume şi istorie. Relativismul moral şi absența oricăror concepții edificatoare privind moralitatea se observă în domeniul cibernetic ca reflexie a condiției omului modern.

Pretextul folosirii supravegherii în masă pentru contracararea terorismului, a fost pus în discuție în fața societății civile sub aspectul *eficienței*, *a rezultatelor obținute* în urma unei astfel de măsuri.

Un exemplu este reprezentat de faptul că după dezvăluirea programului guvernamental de culegere în masă a meta-datelor din telefonia națională realizate de NSA, atât preşedintele Obama B., fostul director al NSA, Heiden M., dar şi câțiva politicieni au afirmat că programul a dus la contracararea a 54 de atacuri[90],

---

[89] Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare,* Oxford University Press, 2017, p. 86.

[90] Cohn C., Kayyali N. *The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible*. Electronic Frontier Foundation 2014.

fapt demontat mai târziu[91]. În acelaşi sens, fostul director tehnic al NSA, a criticat programul de supraveghere în masă sub aspectul productivității scăzute față de alte tipuri de mijloace centrate pe țintele de interes pentru securitatea națională[92], precum programul NSA Thinthread[93].

Un alt program pornit în SUA, prin intermediul NSA, după 11 septembrie 2001, a fost *Stellar Wind*[94] care presupunea folosirea unor instrumente de minare de date din vaste baze de date realizate din comunicații, construite din supravegherea în masă fără autorizație judecătorească.

Programul de supraveghere MUSCULAR (DS-200B)[95] a fost operaționalizat în Regatul Unit de către GCHQ împreună cu NSA şi se baza pe folosirea nodurilor de comunicații prin care erau conectate centrele de date ale operatorilor Yahoo! şi Google[96] şi spre deosebire de alte programe de supraveghere în masă precum PRISM[97] care aveau accesul garantat la centrele de date ale marilor operatori,

---

[91] Medine D. *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. Privacy and Civil Liberties Oversight Board, SUA, 2014, pg. 167.

[92] *Joint Committee on the Draft Investigatory Powers Bill,* William Binney—supplementary written evidence

Marea Britanie, 2016, pp. 180-181.

[93] Proiectul *ThinThread* realizat de NSA în decursul anilor 1990 implica interceptarea şi analiza complexă a datelor obținute, fără a implica o ingerință în viața privată a populației americane. Proiectul a fost înlocuit de *Trailblazer,* în 2002, care nu mai conținea limitările privind viața privată.

[94] În **2012**, publicația americană Wired a făcut public un interviu al unui fost angajat NSA în care vorbeşte de acest program prin care se arăta că practic agenția națională deținea acces la switch-urile importante şi comunicațiile prin satelit ale operatorilor AT&T şi Verizon (Bamford J. *The NSA Is Building the Country's Biggest Spy Center. Watch What You Say*,15.03.2012, Wired). În **2013** Washington Post şi Guardian au dat publicității un raport al Cabinetului Inspectorului General datat martie 2009, dat de Edward Snowden, în care se detaila programul **Stellar Wind**, care încă era aplicat, şi conținea informații despre supravegherea în masă a datelor din telefonie, internet şi e-mail ale cetățenilor americani (Gellman B. *US surveillance arhitecture includes collection of revealing internet, phone metadata.* 16.06.2013 The Washington Post)

[95] Programul de supraveghere în masă se foloseşte de interceptarea fizică a cablurilor prin care funcționează rețelele proprii ale companiilor Google şi Yahoo!, colectând traficul de date vehiculat şi reținându-l pentru câteva zile, perioadă în care cele două agenții guvernamentale extrag informațiile pe care doresc să le utilizeze. Acest tip de program este unul din minim patru astfel de programe existente care se bazează pe un element secundar de siguranță, programe care împreună sunt cunoscute ca **WINDSTOP**(program umbrelă al NSA prin care se realizează colectarea de date indiscriminată în parteneriat cu Regatul Unit, Australia şi Noua Zeelandă care se axează pe traficul de date din Europa şi Asia). *MUSCULAR, 22.07.2015,* Digital Citizenship and Surveillance Society, https://dcssproject.net/muscular/ accesat la 12.01.2020.

[96] Gellman B, DeLong M. *How the NSAs MUSCULAR program collects too much data from Yahoo and Google,* The Washington Post, 28.12.2013.

[97] Program inițiat în **2007** care pune în aplicare prevederile Legii americane împotriva spionajului şi terorismului (Foreign Intelligence Surveillance Act – FISA) pentru a obține meta-datele aferente comunicațiilor pe internet. Existența acestui program a fost făcută publică de Edward Snowden în The Guardian în 06.06.2013.

acesta nu necesita obținerea unei autorizații judecătoreşti[98] pentru accesarea, colectarea şi reținerea datelor.

Similar, Regatul Unit prin programul TEMPORA[99] a plasat 200 de echipamente de interceptare pe cablurile submarine dintre insulele britanice, Vestul Europei şi Statele Unite ale Americii. Serviciul francez de informații DGSE a plasat echipamente de interceptare pe cablurile submarine din zona bazei militare din Djibouti. Serviciul de informații german BND se spune că a instalat echipamente direct în cel mai mare hub de internet din Europa din Frankfurt (DE-CIX). Serviciul de informații Suedez (FRA) are instalate echipamente pe cablurile subacvatice care unesc țările baltice şi Rusia. Serviciile de informații cooperează pentru a culege informații şi a-şi extinde orizonturile pentru a ajunge să acopere internetul[100].

Altă practică folosită, potrivit dezvăluirilor lui Snowden din 2013 sunt programe de tipul Xkeyscore care sunt conectate la platformele de colectare a datelor precum PRISM, care presupunerea extragerea datelor personale ale consumatorilor prin obligarea companiilor private (Google, Microsoft, Apple, Skype) care colectau un volum mare de date în scopuri comerciale, să le transmită în mod regulat serviciilor de informații, fără ştiința utilizatorilor. Această metodă de culegere de informații presupune dorința utilizatorilor de a beneficia de serviciile de stocare în cloud (Microsoft sau Dropbox) şi ignoranța față de colectarea datelor private. Acestea se conexează cu informațiile extrase din platformele de social media, precum Facebook. Astfel de date şi metadate permit maparea relațiilor interpersonale, adresele de IP, conținutul digital transmis, locații geografice şi interese personale. Deci, rețelele diferitelor servicii digitale nu sunt numai naționale, dar şi realizate în parteneriat public-privat[101].

Această stare de fapt, analizată în termeni de actori şi regimul de competență aplicabil, face obiectul unor analize a politicilor publice existente în plan internațional, deoarece datele extrase şi coroborate de serviciile de informații au rolul de a

---

În mod similar, în **1974** New York Times a expus supravegherea masivă realizată de CIA, încălcând regulile ce limitau Agenția în spionajul extern. (Hersh S.M. *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, The New York Times, 22.12.1974), https://perma.cc/FC7V-4WWW accesat la 01.02.2020) Divulgarea din 1974 a dus în anii următori la înființarea unor Comisii de evaluare a activității de informații. **Reforma activității de informații** din SUA de la sfârşitul anilor 1970 **a vizat legalitatea şi transparența.**

[98] Deoarece fac parte din **Programul de supraveghere a terorismului** (început în 2001 şi presupus a fi încetat în 2007) prin care NSA a fost autorizat să monitorizeze, fără obținerea autorizației judecătoreşti, comunicații telefonice, activitatea de pe internet, mesageria şi orice tip de comunicații în care sunt implicate orice persoane considerate a fi în afara SUA, chiar dacă receptorul comunicațiilor se află pe teritoriul american.(Sanger D.E., O'Neil J. *White House Begins New Effort to Defend Surveillance Program*, The New York Times, 23.01.2006).

[99] Utilizat în cooperare cu SUA.

[100] Clarke R.A. *Liberty And Security in a Changing World*, US Review Group on Intelligence and Communications Technologies, 12.12.2013.

[101] Bauman Z., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. *After Snoeden: Rethinking the Impact of Surveillance,* International Political Sociology, nr. 8, 2014, 121-124.

realiza întregirea profilurilor, iar această tehnică trebuie folosită într-un scop justificat, legitim. De aceea împrumutarea acestei tehnici de către mediul privat (cazul Cambridge Analytica[102] şi tehnicile specifice războiul hibrid folosite în alegerile din SUA 2017 şi campania Brexit[103]) în scopul perfecționării campaniilor electorale s-a dovedit a fi o aprigă încercare la adresa democrațiilor europene în 2016-2017.

Un al treilea tip de tehnică de culegere de informații private implică telecomunicațiile, apelurile telefonice, mesajele text, comunicațiile Skype şi diversitatea semnalelor audio video care sunt transmise prin computere, telefoane smart, sateliți şi linii de telefonie fixă. Aceste tipuri de date actualizează constant şi extind aria supravegherii. Odată adunate, atât datele şi meta-datele sunt reținute pentru o perioadă de timp (precum în Tempora) după care se organizează în platforme de integrare precum PRISM pentru a deveni produs informațional inteligibil coroborat cu relațiile interumane pe care le au persoanele suspectate[104].

Un astfel de exemplu este reprezentat de aplicația Exodus[105] dezvoltată de un programator italian care a fost vândută atât serviciului de informații italian, cât şi procuraturii italiene ce are ca obiectiv transmiterea unor numeroase tipuri de metadate ale telefonului infectat, cât şi de înregistrarea convorbirilor şi copierea fotografiilor precum şi a discuțiilor purtate pe aplicațiile Whatsup şi Signal (aplicații care folosesc criptarea mesajelor end-to-end[106]). Aplicația Exodus s-a dovedit a fi folosită neautorizat de unii reprezentanți ai procuraturii italiene, de membrii unei grupări mafiote implicați în defrişări ilegale, dar şi de angajații companiei dezvoltatoare, încălcând dreptul la viață privată a peste 230 de persoane care nu erau vizate de autorități[107].

---

[102] Companie americană de consultanță politică care s-a folosit de un volum masiv de date personale extrase de platforma de social media Facebook coroborate cu tehnici de comunicare strategică în perioada diverselor campanii electorale. (editorial Reuters *Factbox: Who is Cambridge Analytica and what did it do?, 23.03.2018)* A început activitatea în 2013 şi a folosit printre alte mijloace, tehnica microtargeting-ului – marketing direct realizat în urma minării de date private - care implică tehnica de segmentare predictibilă a pieței (analiza cluster).

[103] Lascateu C, *Social media takes a toll on Democracy,* Redefining Community in Intercultural Context, Henri Coandă Air Force Academy Publishing House, 2018, pp. 411-417.

[104] Bauman Z., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. *After Snoeden: Rethinking the Impact of Surveillance,* International Political Sociology, nr. 8, 2014,124.

[105] Aplicația a fost identificată în **2019** în Google Play Store şi a fost dezvoltată de firma *eSurv*, dovedindu-se că datele extrase din telefoanele piratate erau stocate pe un server al operatorului Amazon, în Oregon, de aceea au chemat în judecată compania, pentru transfer neautorizat de date sensibile în afara țării. Atât poliția cât şi procuratura beneficiau de sprijinul operatorilor de telefonie pentru instalarea aplicației, pentru a fi folosită în investigarea cazurilor de corupție, terorism şi mafie.

[106] Criptarea mesajelor *end-to-end* este realizată pentru prevenirea accesului şi modificării mesajelor de altcineva decât emitentul mesajului. Mesajele sunt criptate de emitent, iar terții nu au mijloace de decriptare.

[107] *Government spyware company spied on hundreds of innocent people*, Naked Security, 30.01.2020 https://nakedsecurity.sophos.com/2020/01/30/government-spyware-company-spied-on-hundreds-of-innocent-people/ accesat la 30.10.2020.

Având în vedere faptul că volumul mare de date şi reprezentarea grafică a tiparelor rezultate din intersectarea multiplelor rețele face dificilă distincția dintre străini şi cetățenii proprii, nevoia legalității acțiunilor desfăşurate pune o piedică în funcționarea sistemului, aşadar tendința generală este de a schimba normativul de aşa manieră încât să susțină munca de informații, şi nu o ajustare a sistemului la normele legale. Una din cauzele fundamentale este digitalizarea care determină ca datele adunate din mediul transnațional să facă difuze limitele a ceea ce este național în acest domeniu, la fel şi diferența dintre activitatea de informații şi cea de punere în aplicare a legii. Aceste tendințe încurajează mutarea din tiparul judiciar a procedurilor penale către activități de prevenție şi o abordare bazată pe tipare de predictibilitate, analitice. Aşadar, nu este surprinzătoare apariția unor comportamente neloiale organizațiilor de informații atunci când tendința de simbioză între public şi privat este tot mai accentuată[108].

Revenind la anul **2013**, la nivelul decidenților politicilor europene, odată cu dezvăluirea programului de stocare a datelor numit PRISM, care a fost era în concordanță cu Directiva Europeană[109] privind retenția datelor electronice din comunicații, s-a relevat discrepanța față de prevederile privind protecția datelor cu caracter personal. Prin aplicarea Directivei 2006/24 revenea obligația operatorilor de stocare a acestui tip de date pentru minimum 6 luni şi maximum 24 de luni, iar accesul instituțiilor statului se realiza în baza unei autorizații prealabile. Această directivă a fost abrogată datorită faptului că stocarea în masă a acestor tipuri de date încălca dreptul la viață privată al utilizatorilor, însă aceasta fusese deja transpusă în legislația românească[110] în 2008. Contestată la Curtea Constituțională a României, Legea a fost considerată neconstituțională în ansamblul său[111] şi a fost abrogată la 07.01.2010.

---

[108] Bauman Z., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. *After Snoeden: Rethinking the Impact of Surveillance,* International Political Sociology, nr. 8, 2014, pp. 5-6.

[109] Directiva 2006/24 a Parlamentului European şi Consiliului Europei privind *retenția datelor cu caracter personal generate sau procesate în legătură cu serviciile publice de comunicații electronice sau rețele de comunicații publice*, de completare a Directivei 2002/58/EC privind viața privată şi comunicațiile electronice, **care a fost abrogată în 08.04.2014 prin decizia Curții Europene de Justiție în cauza *Digital Rights Ireland* contra *Irlandei şi alții*** C-293/12 şi C-594/12. Prin efectul acestei directive Poliția şi serviciile secrete ar fi putut să solicite acces la informații precum adresele de IP ori data folosirii e-mail-ului, listingul telefonic, mesageria telefonică.

[110] sub forma Legii nr.298/2008 privind *reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum şi pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice,* **în vigoare de la 20.01.2009 până la 07.01.2010**, abrogată prin decizia Curții Constituționale a României nr. 1258/2009.

[111] În decizia nr. 1258/2009 Curtea reține „În concluzie, având în vedere, în esență, sfera largă de aplicabilitate a Legii nr. 298/2008, raportat la caracterul continuu al obligației de reținere a datelor de trafic şi localizare a persoanelor fizice şi juridice în calitate de utilizatori ai serviciilor de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum şi a altor "date conexe" necesare identificării acestora, Curtea Constituțională constată, pentru motivele mai sus arătate, că

Drept urmare, în urma necesității de implementare a Directivei 2006/24 în statele membre ale Comisiei Europene, în 2012, în România s-a reluat demersul de normare a obligației de stocare a datelor electronice de comunicații de către operatori în forma Legii nr. 82/2012[112] care la rândul ei s-a dovedit a fi neconstituțională în ansamblu în 2014. Curtea Constituțională reține, în esență, că raportat la hotărârea CJUE de abrogarea a Directivei 2006/24, Legea criticată nu mai are un temei juridic din punct de vedere european sau național, statuând că de la data publicării, operatorii nu numai că nu mai sunt obligați să stocheze respectivele tipuri de date, dar nu au nici temei legal pentru acest fapt, sau pentru a le pune la dispoziția instituțiilor statului de ordine şi securitate națională, stocarea fiind limitată la datele necesare facturării serviciilor prestate clienților, cu consimțământul prealabil al utilizatorilor, conform Directivei asupra confidențialității şi comunicațiilor electronice[113].

În plan european, viziunea asupra politicilor de supraveghere în masă în scop preventiv este că nu respectă prevederile Convenției europene a drepturilor omului, aşa cum arată şi avocatul general al Curții de Justiție a Uniunii europene în opinia juridică publicată în ianuarie 2020 privind necesitatea convergenței dintre lege şi mijloacele şi metodele de combatere a terorismului.

Viziunea agreată la nivelul CJUE este că Directiva 2002/58/CE privind viața privată şi comunicațiile electronice exceptează activitățile desfăşurate de autorități în scopul protejării securității naționale de la aplicarea ei, aşadar acestea nu pot obliga operatorii să contribuie la aceste măsuri, fiind afectate interesele comerciale ale celor din urmă. Însă atunci când este necesară un astfel de sprijin din partea companiilor private, care au o serie de obligații legate de respectarea dreptului la viața privată, chiar şi pe considerente de securitate națională, rămâne opozabilă legislația europeană asupra acelor activități, respectiv, protejarea vieții private rămâne obligatorie pentru actorii neguvernamentali. Totodată, se încurajează crearea unui cadru legislativ statal în interesul securității naționale, care să reflecte care sunt activitățile persoanelor care ar putea fi sub incidența autorității de a restrânge drepturile şi libertățile fundamentale[114].

---

legea examinată este neconstituțională în ansamblul ei, chiar dacă autorul excepției individualizează, în special, dispozițiile art. 1 şi 15 din aceasta".

[112] Cunoscută şi ca ***Legea Big Brother,*** Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice şi de furnizorii de servicii de comunicații electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice, **în vigoare din 21.06.2012 până la 19.10.2014,** a fost abrogată prin Decizia Curții Constituționale a României nr. 440/2014**.**

[113] Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice.

[114] Avocatul General Campos Sánchez-Bordona: *the means and methods of combating terrorism must be compatible with the requirements of the rule of law*, comunicat de presă nr. 4/20, CJUE,15.01.2020.

Avocatul General al Curții de Justiție Europene statuează că delimitarea legală a obligației de garantare a confidențialității comunicațiilor şi a traficului de date electronice conexe trebuie interpretată strict şi în concordanță cu drepturile fundamentale din Convenție.

Analizând cazurile conexate *Tele2 Sverige AB* împotriva *Post* şi *Secretarul de Stat pentru Afaceri Interne* împotriva *Watson* şi alții[115] se arată clar faptul că argumentația Curții este împotriva supravegherii realizate fără un scop sau o țintă concretă, considerându-se că, la nivel statal, măsura de a legifera o astfel de activitate nu este conformă dreptului european, iar ca tehnică de culegere de informații este disproporționată. Excepția reprezentată de apărarea securității naționale şi a ordinii publice constă în existența unei rețineri de date axate pe situații clare, pe o perioadă scurtă de timp, şi accesul limitat la aceste date, dar şi în acea situație extraordinară de urgență națională, care ar trebui reglementată, când statele ar putea impune, în mod legitim obligația reținerii tuturor datelor, care ar putea fi atât de extinsă cât se consideră necesar la acel moment. De aceea, în cauza *Tele2/Watson* CJUE a respins ca posibilă măsură legală reținerea generală a datelor personale pentru prevenirea terorismului.

„Lupta împotriva terorismului nu trebuie limitată la eficiența practică, ci în termeni de eficiență legală, de aşa natură că mijloacele şi metodele folosite trebuie să fie compatibile cu condițiile impuse de lege, şi, mai presus, într-o ordine juridică care găseşte protejarea drepturilor omului ca motivare şi scop al existenței sale”[116].

Deopotrivă, Curtea arată într-o opinie premergătoare soluționării cauzei *La Quadrature du Net şi alții*[117] că legislația franceză ***nu*** este conformă Directivei privind viața privată şi comunicațiile electronice, încât persoanele ce au făcut

---

[115] Cauza *Watson* fusese judecată de Curtea Supremă a Marii Britanii în **2016** şi a fost dusă în fața Curții de Justiție a Uniunii Europene în urma hotărârii *Digital Rights Ireland 2019.* Curtea Supremă hotărâse că impunerea operatorilor de telecomunicații să rețină datele de trafic şi conexe pentru **12 luni** nu este conformă cu legislația Uniunii Europene şi nu îndeplinea recomandările cuprinse în cauza *Digital Rights Ireland.* Guvernul britanic a atacat hotărârea, drept urmare, în apel, Curtea Supremă a cerut lămuriri Curții de Justiție Uniunii Europene față de **obligativitatea aplicării hotărârii *Digital Rights Ireland* ca izvor de drept european, aplicabil de drept în legislația națională**. În acest context, CJUE a conexat şi cauza *Tele2 Sverige* (operatorul de comunicații care a încetat reținerea datelor odată cu hotărârea *Digital Rights Ireland* afirmând că legislația suedeză asupra comunicațiilor electronice nu era conformă dreptului european). CJUE a emis o hotărâre preliminară prin care a **arătat că reținerea datelor din supravegherea în masă nu este conformă Convenției europene a drepturilor omului, dacă nu se realizează pentru prevenirea infracțiunilor grave, şi fără proceduri prealabile de autorizare**.

[116] Avocatul General Campos Sánchez-Bordona: *the means and methods of combating terrorism must be compatible with the requirements of the rule of law*, comunicat de presă nr. 4/20, CJUE,15.01.2020

[117] Cauza CJUE 511/18 (în curs de judecare). Reclamantul este o organizație franceză privind apărarea dreptului la viață privată pe internet, dar şi pentru libertatea circulării informației pe internet, ca drept la libertatea de exprimare. Obiectul cauzei este reprezentat de legislația franceză datând din 2006, care oferă posibilitatea legală a stocării generale a datelor din comunicații de către operatori.

obiectul procesării datelor de către autorități nu sunt notificate pentru a beneficia de o justă cale de apărare. Pe de altă parte, Directiva nu interzice reținerea datelor şi localizarea persoanelor în timp real dacă măsura este prevăzută în cadrul procedurilor legale de acces legitim la datele reținute şi fac obiectul aceleiaşi protecții.

3. CULEGEREA DE INFORMAȚII DIGITALE – PERSPECTIVA CONSECINȚIALISTĂ

Instituțiile guvernamentale au atât rolul de a proteja drepturile cetățenilor, cât şi rolul de utilizatori, potrivit intereselor legitime în dezvoltarea *ştiințelor sociale computaționale*[118]. Acestea nu numai că dețin volume mari de date guvernamentale, dar şi orice date deținute de companiile private care activează în domeniul de jurisdicție al statului trebuie să comunice orice dată deținută în baza unei solicitări legitime. Majoritatea statelor mențin un echilibru între nevoia de acces la informații a instituțiilor statului, prin organele de punerea în aplicare a legii sau pentru rațiuni ce țin de securitate națională, şi dreptul cetățenilor la viață privată. În țările democratice în care funcționează statul de drept, accesul organelor de aplicare a legii la datele din comunicații de la operator se face în baza autorizației emise de un judecător, în temeiul unei motivații rezonabile (în țări precum China şi Iran[119], accesul autorităților la astfel de date se realizează direct)[120].

Colectarea la scară largă, păstrarea, agregarea, folosirea şi difuzarea a informațiilor private (date personale filtrate, complexe, localizate geografic) oferă un instrument social eficient care poate naşte şi posibilitatea unor abuzuri. Importanța acestui instrument rezidă în faptul că, prin intermediul rețelelor de socializare, industria operatorilor de servicii, cercetătorii dar şi instituțiile statului accesează mecanismul de identificare a curentelor comportamentale ale populației, precum şi profilul individual al unui singur utilizator[121].

Datele utilizatorilor odată adunate de companiile private pot fi accesate de orice instituții sub a cărei jurisdicție se află activitățile companiei. Problema de etică care se pune este că *scopul culegerii de date personale* de către operatorul privat este diferit față de scopul urmărit de către instituțiile statului.

---

[118] Denumire acordată domeniului interdisciplinar dintre *analiza de date specifică informaticii*, şi *adunarea volumelor masive de date private specifică ştiințelor sociale*.

[119] Whitehead T., *New powers to record every phone call and email makes surveillance '60m times worse*, Telegraph, 2012.

[120] Oboler A., Welsh K., Cruz L. *The danger of big data: Social media as computational social science,* First Monday, 2012.

[121] Lascateu C., *Social media takes a toll on Democracy, Redefining Community in Intercultural Context*, Henri Coandă Air Force Academy Publishing House, 2018.

Declasificat în 22 martie 2018 de către Camera Reprezentanților din Senatul Statelor Unite ale Americii, *Raportul comunității de informații privind măsurile active ruseşti*[122], prezintă în detaliu faptul că începând cu anul 2015, Rusia a avut drept scop manipularea alegerilor prezidențiale din SUA, în principal prin aplicarea în spațiul cibernetic a tehnicilor informative perfecționate după încheierea celui de-al Doilea Război Mondial[123]. Investigațiile au început în ianuarie 2017 şi au fost menite să clarifice rolul jucat de *campania de influență informativă a Rusiei în spațiul cibernetic* şi dacă au fost țintite SUA şi aliații săi cu scopul de **a submina încrederea populației în procesul democratic**[124].

În prezent, resursele pe care Kremlinul le utilizează în operațiunile informative externe sunt atât de origine statală, cât şi non-statală. Aceasta presupune abordarea comprehensivă şi folosirea concertată a resurselor comunității de informații, cu cele ale mass-media, social-media (incluzând şi troli), companii private şi publice care aderă la viziunea politică rusească, grupări de crimă-organizată, ONG-uri, (think-tancuri şi fundații), grupuri sociale şi religioase[125]. Unul din scopurile urmărite pe termen scurt este de a scade încrederea în decidenții politici şi în instituțiile democratice, în procesul electoral şi mijloacele de informare independente, dar pe termen lung, să slăbească coeziunea socială pentru a adera ulterior la ideologia Kremlinului[126].

---

122 Raportul arată cum s-au desfăşurat măsurile active din Rusia în ultimii ani şi subliniază metodic procesele implicate oferind recomandări pentru prevenirea în plan strategic, atât la nivel de politici guvernamentale cât şi ca implementare de soluții de securitate cibernetică. (House Permanent Select Committee on Intelligence, *Report on Russian Active Measures*, U.S. House of Representatives, Washington, 2018).

123 Guvernul Rusiei foloseşte de mult timp activitățile de propagandă combinate cu tehnici ale serviciilor informații, diplomație şi asertivitate politică pentru a-şi atinge obiectivele (Bittman L., *The KGB and Soviet Disinformation: An Insider's View*, Washington: Pergamon-Brassey's, 1985, pg.43) şi îşi exercită puterea de influență prin intermediul **unor terți**. Termenul de ***măsură activă*** este de fapt traducerea din limba rusă a *aktivnyye meropriatia* care a fost folosită de KGB (Komitet Gosudarstvennoy Bezopasnosti sau Comitetul pentru Securitate de Stat) pentru multe din activitățile de influență utilizate în timpul Războiului Rece (Departamentul de Stat al SUA, *A Report on Active Measures and Propaganda*, 1986 - 1987, Department of State Publication, 1987, pg. viii). Alții specialişti au definit măsurile active ca *tehnici sovietice de influență pentru a determina modul în care percepția publică şi decidenții politici se comportă favorabil față de sovietici şi negativ față de oponenții lor*, denumit şi *managementul percepției*.

124 În manualul serviciilor de informații militare ruse: „Războiul psihologic există de când este omenirea" (Kovalev A., Bodner M., *The Secrets of Russia's Propaganda War, Revealed*, The Moscow Times, 2017).

125 Parlamentul European a adoptat Rezoluția 2016/2030 prin care adresează şi recunoaşte o gamă largă de metode şi instrumente pe care le foloseşte Rusia pentru a disemina ***dezinformarea şi propaganda*** (European Parliament Resolution, *EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties*, 2016/2030).

126 Galeotti M., *Controlling Chaos: How Russia Manages its Political War in Europe*, European Council on Foreign Relations, 2017.

Importanța comunicării strategice şi necesitatea de a contracara dezinformarea depinde de precizia evaluării tipurilor de amenințări şi de realitățile din mediul internațional[127]. „Multe state consideră capabilitățile cibernetice o parte legitimă şi necesară din setul lor de instrumente strategice, alături de diplomație, influență economică şi putere militară(...) Acest lucru necesită implicarea factorilor de decizie şi identificarea măsurilor care să împiedice conflictele generate utilizarea acestora"[128].

Drepturile fundamentale la viața privată şi la protecția datelor cu caracter personal ar trebui să joace un rol crucial în politica fiecărui Legiuitor pentru a ține pasul cu astfel de evoluții, iar autoritățile independente de protecție a datelor personale consideră acest ***obiectiv de legiferare o prioritate strategică***. În 2005, *Rezoluția de la Montreux privind utilizarea datelor cu caracter personal pentru comunicarea politică* a subliniat faptul că autoritățile de reglementare în domeniul protecției datelor au identificat o creştere a prelucrării acestor date de către **actori necomerciali**, făcând trimitere la analiza „datelor sensibile legate de convingeri politice sau morale şi intenții de vot" şi la „profilul psihologic-comportamental al unor persoane, realizat prin mijloace invazive, pentru a fi catalogate ca simpatizante, susținătoare, sau adepte ale unor idei politice". Rezoluția din 2005 a solicitat comunității internaționale să ***emită şi să aplice normele*** privind protecția datelor, minimizarea lor, prelucrarea legală, existența consimțământului, transparența vehiculării datelor, drepturile persoanelor vizate, stabilirea scopului de prelucrare şi securitatea datelor[129].

Departamentul de Stat al SUA subliniază că eforturile Rusiei de a influența alegerile şi referendumurile din Europa includ „atât deschis, cât şi în mod secret, sprijinirea partidelor politice de extremă dreapta, dar şi cele de stânga, finanțarea grupurilor de lobby şi a ONG-urilor, precum şi efectuarea de investiții mici, în sectoare economice cheie *pentru a construi o influență politică în timp*, şi pentru ca tehnicile folosite „să se concentreze asupra exploatării conflictelor ideologice naționale pentru a deteriora consensul democratic centrat asupra instituțiilor de bază"[130] – alegeri libere, stat de drept, respectarea drepturilor omului şi transparență decizională[131].

---

[127] Schoen F., Lamb J. C., *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Strategic Perspectives, 2012, pp. 117-118.

[128] Declarația lui Ben Hiller, Cyber Security Officer al OSCE Secretariat's Transnational Threats Department la prima întâlnire a grupului de lucru privind măsuri de cooperare şi creştere a încrederii în spațiul cibernetic organizată de Organizația Statelor Americane, Washington DC la 02.03.2018 (OSCE, *OSCE shares experiences with Organization of American States on how to enhance interstate co-operation, transparency, predictability and stability in cyberspace*, 2018).

[129] European Data Protection Supervisor, *Online manipulation and personal data*, *Opinion*. 3, 2018, p. 5.

[130] U.S. Department of State. (November 7, 2017) *Report to Congress on Efforts by the Russian Federation to Undermine Elections in Europe and Eurasia, Pursuant to the Countering America's Adversaries through Sanctions Act of 2017*, U.S. Department of State Publishing House 07.11.2017.

[131] Lascateu C., *Obiectivele Războiului hibrid rus,* Geopolitica, anul XVI, nr. 74 (2/2018).

În aceeaşi notă, un studiu realizat de Alianța pentru Asigurarea Democrației a Fondului german Marshall arată că Guvernul rus a folosit atacuri cibernetice pentru a realiza operațiuni ample de dezinformare şi campanii de manipulare financiară menite să intervină în afacerile interne a cel puțin 27 de țări europene şi nord-americane începând cu 2004[132].

În acest context, se relevă faptul că măsurile din domeniul securității naționale care privesc atât cetățenii cât şi mediul economic privat pot fi definite ca fiind acele mijloace tehnice şi strategice care au fost inițiate cu scopul de a preveni materializarea amenințărilor la securitatea națională, indiferent dacă sunt provenite de la cetățeni sau străini, ori din exterior de la un alt stat, sau actor non-statal. În securitatea națională sunt incluse prioritățile guvernamentale fundamentate de un interes național, iar măsurile adoptate în plan tehnologic au rolul de spori securitatea națională, dar şi de a menține nivelul de protecție existent, chiar dacă nu sunt puse în discuție publică suficient de mult[133].

3.1. Spațiul virtual o resursă pentru interesul național

Având în vedere că domeniul securității naționale, din punctul de vedere al încadrării juridice, înglobează o serie de zone ale legalității de la drept penal special, la mecanisme sancționatorii administrative (expulzarea, conferirea statutului de persona-non-grata sau nepermiterea intrării în țară), la restrângerea unor drepturi şi libertăți în afara cadrului procesual penal. Totodată, aria juridică a securității naționale acoperă şi în mod special culegerea de informații şi formele specifice de supraveghere, dar şi dreptul internațional al conflictelor armate. Fiecare din aceste zone de competență cuprind aceleaşi provocări de punere în aplicare a normativului[134] la fel ca multe alte subdomenii din dreptul administrativ, mai exact, față de obținerea unui *grad ridicat de precizie în limbajul*[135] care

---

[132] Țările incluse sunt Belarus, Bulgaria, Canada, Cipru, Republica Cehă, Danemarca, Estonia, Finlanda, Franța, Georgia, Germania, Ungaria, Italia, Letonia, Lituania, Macedonia, Moldova, Muntenegru, Norvegia, Polonia, Portugalia, Spania, Suedia, Turcia, Regatul Unit, Ucraina şi Statele Unite (Dorell O., *Alleged Russian Political Meddling Documented in 27 Countries Since 2004*, USA Today, 2017).

[133] Michael M.G., Michael K., *National Security: The Social Implications of the Politics of Transparency,* University of Wollongong, 2006.

[134] Din fr. *normatif,* ansamblu de norme, instrucțiuni, proceduri, îndrumări, dispoziții cu privire la un domeniu de activitate, dar şi reguli de conduită care au caracter de normă (Dicționarul explicativ al limbii române, ed. 2, Academia Română, Institutul de Lingvistică, Univers Enciclopedic Gold, 2009)

[135] Limbajul juridic - reprezintă atât un lexic aparte, specializat, prin care cuvintele cu sens comun capătă sens juridic, dar şi termeni juridici prin excelență, care servesc scopului de a conferi claritate, precizie şi accesibilitate pentru oricare destinatar, fiind specific ştiinței sociale reprezentate de drept. (Sferle A. *Limbajul juridic şi limba comună,* Universitatea Tibiscus Timişoara, Universite Paris III Sorbonne Nouvelle, 2005)

dă forma reglementării activității pentru obținerea rezultatelor optime fără a încălca nejustificat libertatea personală, viața privată şi alte interese private ale persoanelor[136].

Dacă ne raportăm la cazul particular al reglementării[137] spațiului cibernetic, problema limbajului juridic privind stabilirea naturii juridice şi a dreptului aplicabil acestui spațiu s-a rezolvat prin prisma exercitării puterii statale, manifestată în principal raportat la suveranitatea teritorială, prin legi naționale.

În contrast, depăşind aria teritorialității[138], şi axat exclusiv din punct de vedere pe dezvoltare digitală, serviciile de informații statale s-au pregătit constant pentru folosirea resurselor informaționale reprezentate de inovațiile din acest spațiu, chiar dacă terminologia juridică națională nu este în concordanță, sau nu a definit în mod expres raporturile juridice ce se nasc din folosirea acestei resurse, dar nici efectele juridice determinate de aceste raporturi juridice, atât în plan național cât şi în relațiile cu alte state.

În plan internațional, analizând mozaicul de reglementări naționale privind spațiul virtual, se remarcă faptul că există o zonă liberă de norme şi cutume pentru anumite tipuri de activități precum cea de *culegere de informații digitale*.

Nevoia de reglementare la nivel interstatal apare în contextul în care pot apărea derapaje în manifestarea intereselor naționale, ca expresie a nevoii de a sancționa comportamentul reprobabil al statelor-națiune în acest plan existențial, sau de a justifica legitima-apărare. O formă de drept cutumiar este reprezentat de Manualul de la Tallinn 2.0 privind dreptul aplicabil operațiilor în spațiul cibernetic din 2017[139] – ca formă revizuită a celui inițial privind războiul cibernetic din 2013[140] – realizat prin efortul experților Organizației Tratatului Atlanticului de Nord (NATO) de a sintetiza totalitatea normelor de drept aplicabile în cazul conflictelor

---

[136] Hafetz J., *A Problem of Standards? Another Perspective on Secret Law,* William & Mary Law Review, vol. 57, 2016, p. 14.

[137] A supune la o normă sau un regulament, a stabili raporturi legale, a pune în ordine, sau, un ansamblu de norme juridice aplicabile unui domeniu, sau, operație de stabilire a acestor norme.(Dicționarul explicativ al limbii române, ed. 2, Academia Română, Institutul de Lingvistică, Univers Enciclopedic Gold, 2009)

[138] „**Teritoriul** este unul din elementele constitutive ale statului, împreună cu populația şi organizarea politică, de aceea art. 3 din Constituția României prevede că *teritoriul este inalienabil* iar apărarea sa este o problemă de securitate națională. Apărarea teritoriului priveşte nu numai forțele armate, statul în general, dar şi fiecare cetățean în parte. În acest sens, respingerea oricărei agresiuni este o problem de interes național." (Constantinescu M. Iorgovan A. Murau M. Tănăsescu E.S. *Constituția României revizuită comentarii şi explicații,* All Beck, 2004, p. 5).

[139] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, ed. 2, Cambridge University Press, 2017. Acest ghid, extinde practicile guvernamentale din spațiul cibernetic în afara dreptului internațional umanitar, deci la **aplicarea pe timp de pace**.

[140] *Tallinn Manual on the International Law Applicable To Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013.

din acest spaţiu virtual, echivalate cu un atac armat precum este definit în dreptul internaţional umanitar.

Nu este un demers unanim acceptat în mediul internaţional, dintre cei mai fervenţi opozanţi fiind Rusia şi China, care argumentează caracterul subiectiv al documentului menţionat ca fiind reprezintă o emanaţie a culturii vest-europene care nu poate fi impusă tuturor naţiunilor, cu aplicare universală[141].

Deci, aceşti teoreticieni care au pus piatra de temelie în adoptarea unei linii juridice a activităţilor desfăşurate în spaţiul cibernetic pe timp de pace, au propus ca fundament pentru reglementarea spaţiului cibernetic formele de interpretare juridică precum analogia şi paralelismul legal privind şi alte tipuri de raporturi juridice internaţionale ca dreptul mărilor, dreptul comunicaţiilor sau dreptul spaţial, care izvorăsc din tratate ca formă juridică a cutumelor prestabilite de-a lungul istoriei, pornind de la faptul că acest spaţiu nu aparţine niciunui unui stat, ci reprezintă o resursă la care sunt îndreptăţite să participe toate statele, în universalitatea lor.

Însă, chiar dacă viziunea juridică asupra spaţiul cibernetic (cum rezultă din Manualul Tallinn 2.0) este de a-l cataloga ca a „cincea" jurisdicţie, alături de spaţiile obişnuite, pământ, mări, aer şi spaţiu, se impune observaţia că o analogie de acest tip comportă şi o serie de limitări în interpretarea logică.

Pe când celelalte patru domenii consistă în lucruri tangibile, spaţiul cibernetic este, printr-o încercare de comparaţie, **un mediu unic** în care electronii şi fotonii, prin interacţiunile determinate de părţi binare de cod informatic, dictează forma şi structura „obiectelor" şi „evenimentelor". Acest spaţiu virtual seamănă mai degrabă cu plasma ce înconjoară planeta, întrucât amândouă sunt fenomene electromagnetice cu reacţie imediată pe distanţe foarte mari. Dar nici această comparaţie nu este exactă, chiar dacă, în esenţă, în ambele spaţii comparate este dificil de stabilit „unde" sunt poziţionate „obiectele" în spaţiul cibernetic, întrucât sunt continue şi aproape instantanee[142].

Totodată, spaţiul cibernetic este de cele mai multe ori înţeles ca sinonim al *internetului* sau al *world wide web,* dar domeniul cibernetic este mult mai extins de atât, incluzând partea fizică a tehnologiei, orice instrument conectat la internet (thumb drives, imprimante, laptopuri, televizoare care se conectează la internet prin alte echipamente, cabluri sau reţele wireless, telefoane care operează pe diferite frecvenţe, comunicaţii prin satelit, GPS, dar şi alte obiecte convenţionale precum navigaţia din automobile sau sistemele de monitorizare şi securitate de la bordul avioanelor, sau echipamentele de uz casnic care pot fi controlate prin telefoanele smart)[143].

---

[141] Arredy J.T. *China Aims to Rewrite Rules of Global Web,* Wall Street Journal, 2015.

[142] Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare,* Oxford University Press, 2017, p. 17.

[143] Dipert R.R. *The Essential Features for an Ontology for Cyberwarfare, Conflict and Cooperation in Cyberspace,* CRC Press, 2013, pp. 35-48.

Această întreagă rețea cibernetică, de multe ori numită *the Internet of Things (IoT)* – internetul lucrurilor – este într-o constantă creştere şi include deopotrivă drone şi alte echipamente pilotate de la distanță, tehnică militară fără prezența umană, partea fizică a echipamentelor precum şi sistemele de operare care le dirijează şi comunică cu centrele de comandă, şi care de fapt monitorizează şi guvernează internetul în sine[144].

În acest spațiu, o tranzacție simplă cum este trimiterea unui e-mail sau apelarea unui număr de telefon, sau plata on-line a unei facturi reprezintă un „obiect" – cum este e-mailul – şi „evenimentul" adiacent – trimiterea şi primirea mesajului. Aceste operațiuni înglobează părți care interacționează în multe diferite părți ale lumii, de-a lungul a mai multor țări şi continente simultan[145].

Şi totuşi, din punct de vedere guvernamental, statele întreprind demersuri ca să mențină şi să extindă o serie de sisteme informatice şi tehnologii interoperabile, pentru a reduce cheltuielile şi a optimiza partea administrativă a datelor electronice[146].

Însă, folosirea operațiunilor cibernetice este de generație nouă la fel cum este şi folosirea pârghiilor economice pentru a dirija politica guvernelor străine. Un exemplu elocvent este reprezentat de tacticile războiului hibrid purtat de Rusia care îmbină strategiile politicii de stat cu tacticile informative ale serviciilor de informații în spațiul cibernetic. Datorită faptului că expansiunea tehnologiei şi a rețelelor de socializare au reprezentat o resursă variată de informații care generează costuri minime, riscuri relativ minimale şi rezultate bune. Utilizarea strategiilor hibride nu este o noutate în cazul Rusiei. În epoca sovietică, Moscova folosea în mod frecvent tactici subversive pentru a câştiga influență şi a modela peisajul politic european[147].

Războiul hibrid[148] în sine este modelul empiric de aplicare a principiilor consecințialismului în activitatea de informații din spațiul cibernetic, deoarece în această viziune primează atingerea scopului şi mai puțin etica mijloacelor folosite.

---

144 *Is More Gridlock Just a Hack Away?* Washington Post, 09.08.2015.

145 Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare,* Oxford University Press, 2017, p. 18.

146 Ca parte a implementării strategiei Comisiei Europene de *E-Government.*

147 Lascateu C., *Obiectivele Războiului hibrid rus*, Geopolitica, anul XVI, nr. 74 2/2018.

148 Mai mulți termeni conecşi celui de *război hibrid* sunt „strategii din zona gri", „competiție la limita conflictului", „măsuri active" şi „război de generație nouă". Deşi diferențele sunt subtile toți aceşti termeni indică acelaşi lucru: Rusia foloseşte mai multe instrumente de putere şi influență, cu accent pe instrumente non-militare **pentru a-şi urmări interesele naționale în afara granițelor**. Dacă vorbim de războiul hibrid purtat de Rusia în ultimii ani ne referim la implementarea unei game variate de instrumente, dintre care multe nu sunt militare pentru a facilita intereselor naționale ruseşti. Moscova caută să folosească războiul hibrid pentru a garanta reuşita unor politici de stat precum divizarea şi slăbirea puterii exercitate de NATO, subminarea guvernelor prooccidentale pentru a crea pretexte pentru război, anexarea de teritorii şi asigurarea accesului la piețele europene în condițiile proprii. Creşterea folosirii strategiilor hibride de ruşi, din ultimii ani, este o expresie clară a

3.2. Elemente consecinţialiste în culegerea de informaţii private digitale – obiectivele războiul hibrid rus

În timp ce tehnologia asigură influenţă politică ca instrument de soft-power şi tactici precum campaniile deschise de dezinformare, democraţiile se adaptează la o nouă formă de existenţă fără a ajunge în stări de criză generatoare de conflicte armate[149].

Ca reper temporal, tehnicile integrate de informaţii au fost folosite timpuriu de Rusia[150]. Dacă analizăm demersurile statale ce preced invazia trupelor ruseşti din Cecenia în 1999, Georgia în 2008, Ucraina în 2014 sau Siria în 2015, aceste conflicte reflectă un tipar în care Kremlinul porneşte mici războaie similare ca mod de acţiune, pentru a-şi întări obiectivele politice interne, dezvăluind o legătură directă între agresiunile externe ale guvernului rus şi opresiunea internă[151].

Pentru a înţelege tacticile folosite de Kremlin[152] în plan extern de subminare a democraţiei trebuie menţionat că acestea au fost folosite întâi în plan intern, iar aplombul şi brutalitatea lor a crescut în timp[153].

Comunitatea de informaţii din Rusia este implicată într-o campanie asertivă de susţinere a viziunii şi intereselor geopolitice ale Kremlinului, folosind pe lângă spionaj, măsuri active concertate către subminarea şi destabilizarea altor actori guvernamentali occidentali. Moscova a dezvoltat servicii de informaţii diferite pe care le poziţionează într-o permanentă competiţie, a căror competenţe se întrepătrund, în scopul de a se încuraja operaţiunile informative riscante şi deţinerea de

---

expansiunii capabilităţilor militare ruseşti în concordanţă cu atitudinea antagonistă Vestului manifestată de Kremlin. Chivvis C.S., *Understanding Russian "Hybrid Warfare" and What Can Be Done About it*, RAND Corporation, CT-468, Testimony presented before the House Armed Services Committee 22.03.2017).

149 Lascateu C., *Social media takes a toll on Democracy*, Redefining Community in Intercultural Context, Henri Coandă Air Force Academy Publishing House, 2018.

150 În 1903 **Vyacheslav Plehve,** ministrul afacerilor interne al Ţarului Nicolaie remarcă: „suntem în ajunul unei revoluţii" şi „pentru a evita o revoluţie, avem nevoie de o mică victorie de război" pentru a „distrage atenţia maselor" cu un an înainte ca Imperiul Ţarist să intre într-un război dezastruos cu Imperiul Nipon. Remarca citată a fost făcută după înăbuşirea unei greve în Odessa. El tocmai transformase Ohkrana (poreclă dată serviciului de securitate) în cea mai sofisticată poliţie secretă din lume. (Montefiore S., *The Romanovs*, Knopf A.A., 2016, p. 510-514). Lenin adoptase metodele *Ohkrana* când a înfiinţat Cheka, predecesoarea NKVD-ului Stalinist, care a devenit KGB mai târziu şi este reîncarnarea actualului FSB. (Fischer B., *Okhrana: The Paris Operations of the Russian Imperial Police*, Diane Publishing,1999, p. 10).

151 Baer D.B., Declaraţia depusă în faţa Senatului SUA – Comitetul pentru Relaţii Externe - intitulată *The European Union as a Partner Against Russian Aggression: Sanctions, Security, Democratic Institutions and the Way Forward,* 04.04.2017.

152 O expresie a punerii în act a *doctrinei Gherasimov* - o combinaţie letală între atacuri militare convenţionale, asasinate, campanii de dezinformare, atacuri cibernetice şi transformarea în arme a corupţiei şi energiei.

153 A Minority Staff Report Prepared for The Use of The Committee on Foreign Relations United States Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, U.S. Government Publishing Office, Washington, 10.01.2018.

sursele de informații variate. Pe când **colectarea de informații este masivă**, aparatul de analiză este limitat, aşadar capacitatea acestei politici externe hibride de a influența relațiile internaționale şi politica globală nu poate fi negată[154].

Ştirile false şi trolii de pe Internet au fost folosite de Kremlin ca tehnici de manipulare concertate şi asupra populației, cu precădere după protestele anti-Putin din 2011-2012[155]. Concentrat pe controlul social-media şi a platformelor online folosite de opoziția politică a puterii unde se propagau suspiciunile de fraudă electorală şi se încurajau mobilizarea protestatarilor, **Kremlinul a folosit produse software pentru a monitoriza online opinia publicului.** Ca răspuns, a recurs la metode de inundare a social media cu propria viziune, plătind bloggeri să plaseze materiale pro-Kremlin în postări irelevante politic[156]. În 2014, după câştigarea alegerilor de către Putin, Legiuitorul rusesc a recurs la a acorda legitimitate instituțiilor pentru blocharea site-urilor care deținеau „materiale extremiste" sau reprezentau o „amenințare la adresa publicului" fără existența unei hotărâri judecătoreşti[157].

Mai mult, în 2015, a intrat în vigoare o lege potrivit căreia companiile străine care activează pe teritoriul Rusiei *sunt obligate să țină toate datele provenite de pe teritoriul țării pe servere localizate în țară*, sub pretextul oferirii unei mai bune protecții, demers care este circumscris încercării de a controla conținutul corespondenței electronice şi social media a propriei populații[158]. Confruntat cu faptul că operatorii străini au refuzat să se conformeze, guvernul rus a ordonat providerilor locali de Internet să blocheze LinkdIn şi a amenințat că va restricționa accesul la Facebook în 2018 dacă nu se conformează[159]. Similar, serviciile secrete şi-au manifestat influența asupra conducerii VKontakte[160] pentru a dezvălui informații despre protestele din Ucraina pe Euromaidan şi activiştii anti-corupție din Rusia. Conducerea platformei a fost înlocuită cu oligarhi apropiați viziunii lui Putin[161].

În acelaşi timp, Kremlinul a dirijat şi sponsorizat hackeri pentru a infiltra conturi de e-mail ale oponenților politici, o serie de jurnaliști şi cel puțin 100 de

---

154 Galeotti M., *Putin's Hydra: Inside Russia's Intelligence Services*, London: European Council on Foreign Relations (ECFR), 2016.

155 Potrivit investigațiilor jurnalistice realizate de publicația The New York Times.

156 Chen A., *The Agency*, The New York Times, 02.06.2015.

157 rezultând în blocarea a 3 site-uri de ştiri ale opoziției şi blogul activistului Alexei Navalny *(Russia Censors Media by Blocking Websites and Popular Blog*, The Guardian, 14.03.2014).

158 *Russia Passes Law to Force Websites onto Russian Servers*, Reuters, 04.07.2014.

159 Khrennikov I., *Russia Threatens to Shut Facebook Over Local Data Storage Laws*, Bloomberg Technology, 26.09.2017.

160 Platformă social media folosită în spațiul ex-sovietic.

161 Soldatov A., Borogan I., *The Red Web: The Kremlin's War on the Internet*, PublicAffairs, 2015, pp. 291-294.

persoane reprezentative pentru societatea civilă din Rusia – un semnal că tacticile eficiente în plan intern vor putea fi extinse împotriva ţintelor internaţionale[162].

Caracteristicile războiului hibrid rus[163]	
Utilizează la minimum forța armată convențională	Pentru a evita o confruntare directă cu forțele aliate NATO Moscova îşi urmăreşte interesele fără a folosi forța armată, dar asta nu înseamnă că nu foloseşte în mod deschis ca strategie amenințarea utilizării armelor convenționale sau chiar nucleare.
Este persistent	Războiul hibrid desființează concepția tradițională de război sau pace. Realitatea războiului hibrid este că intensitatea conflictului fluctuează, uneori devenind conflict armat, însă strategiile hibride sunt în permanență în curs de implementare.
Se axează pe populație	Experiența ultimelor războaie purtate de Statele Unite şi aliații săi în Balcani şi în orientul mijlociu în ultimele decenii i-au convins pe decidenții Moscovei de importanța abordării unei strategii care să influențeze populația țărilor vizate prin operațiuni informaționale şi grupuri afiliate. Rusia foloseşte războiul hibrid pentru a atinge obiectivele proprii în sisteme politice şi sociale existente

Astfel de fenomene determină reacții în plan internațional, politicile fiind îndreptate către alocarea de resurse financiare suplimentare pentru colectarea de date şi analiză informațională, întrucât alertarea preventivă asupra activităților de tipul celor desfăşurate de Rusia este foarte importantă, dar nu poate acapara întreaga activitate a capabilităților de strângere şi analiză a datelor şi informațiilor într-un stat.

Operațiunile externe de manipulare duse de Rusia şi activitățile circumscrise războiului hibrid au dus, în mod inerent, la sancțiuni internaționale, atunci când Rusia a anexat ilegal Crimeea şi susținut financiar şi politic regimul din regiunea

[162] Satter R. şi alții, *Russia Hackers Pursued Putin Foes, Not Just US Democrats*, Associated Press, 02.11.2017.

[163] Tabel realizat pe baza concluziilor lui Chivvis C.S. în *Understanding Russian „Hybrid Warfare" and What Can Be Done About it*, RAND Corporation, CT-468, Testimony presented before the House Armed Services Committee 22.03.2017.

separatistă Donbas din estul Ucrainei. Sancțiunile au continuat să fie aplicate de Uniunea Europeana şi S.U.A. ca răspuns la atacurile cibernetice, încălcări ale drepturilor omului sau corupție.

Relevant este, în perspectiva analizei realizate, că aceste campanii de influență se dovedesc a fi eficiente şi greu de contracarat, chiar dacă instituțiile şi reprezentanții media din Europa întreprind măsuri pentru a aborda şi a atenua amenințarea reprezentată de campaniile online de manipulare a opiniei publice, punerea în aplicare a legilor privind confidențialitatea persoanelor şi finanțarea organizațiilor de securitate cibernetică.

3.3. Elementele consecințialiste în culegerea de informații private digitale - excepționalismul

Acest discurs moral din sfera securității naționale privind faptul că *atingerea scopului nu face importante mijloacele folosite* este dificil de catalogat, putând fi denumit „o moralitate a excepțiilor" sau „etica exigențelor" sau chiar „o pledoarie pentru pretexte" sau „o cerere de exceptare" pentru că, în mod particular, un astfel de raționament şi lista condițiilor necesare pentru încuviințarea unei exceptări, sau pentru recunoaşterea situației excepționale, se regăseşte în multe ale tipuri de discurs moral (precum cel al deontologiei sau cel realist) şi mai ales de logică juridică precum cele din dreptul penal referitoare la dreptul de auto-apărare, sau cele din plan contractual atunci când vorbim de cazul fortuit, sau, în caz de război când vorbim de situații de urgență, întotdeauna aceste evenimente sunt strâns legate de *alte condiționări* pentru a stabili caracterul rar şi neobişnuit[164].

În toate situațiile de raționament moral de acest fel, dar şi juridic, se regăsesc şi cerințele unei ***juste cauze*** alături de o formă de *asumare legitimă a autorității acordării acelei excepții*. Totodată, în aceste circumstanțe se identifică şi faptul că normele morale dominante în astfel de situații de securitate națională presupun folosirea unei *soluții excepționale* doar în ultimă instanță pentru a diminua pagubele inutile asupra altor agenți morali relevanți (cum ar fi în dreptul umanitar limitarea numărului victimelor colaterale).

Totuşi, s-a relevat o tendință internațională de a opaciza problemele apărute din activitățile de informații, tradiționalul scrutin public căpătând o importanță diminuată față de predilecția implementării de proceduri juridice bazate pe *delegarea cunoaşterii depline* către oficiali ce au aviz de securitate[165].

---

[164] Coleman S. *Even dirtier Hands in War: Considering Walzer s Supreme Emergency Argument,* Research in Ethical Issues in Organisations, pp. 61-73.

[165] Bigo D. *Raportul privind securitatea națională şi probele secrete în legislație şi în fața instanțelor: explorarea dificultăților* Comisia Parlamentului European pentru libertăți civile, justiție şi afaceri interne (LIBE), 2014.

Rezoluția Adunării Generale a Organizației Națiunilor Unite referitoare la *Dreptul la viață privată în Era Digitală*, nr. 68/167 din 21.01.2014, aduce o interpretare nouă statuând că „supravegherea extrateritorială şi/sau interceptarea comunicațiilor, dar şi colectarea de date cu caracter personal, mai ales atunci când sunt realizate la scară largă, pot afecta exercitarea drepturilor omului", deoarece „aceleaşi drepturi pe care le au oamenii offline, trebuie protejate on-line, incluzând dreptul la viață privată", cerând statelor să „respecte şi să protejeze dreptul la viață privată, chiar şi în contextul comunicațiilor digitale", aceasta fiind o recomandare de schimbarea politicilor naționale în ceea ce priveşte operatorii de comunicații.

Elementul de noutate este reprezentat de extinderea aplicării normelor tratatelor internaționale la care au aderat anumite state, în plan extrateritorial, deci o extensie a jurisdicției drepturilor omului ca autoritate asupra indivizilor, indiferent de spațiul în care se află, sau forma de guvernământ a statului în care se află.

Aceasta suplimentează prevederile Convenției pentru apărarea drepturilor omului şi a libertăților fundamentale[166] care debutează prin a stabili *jurisdicția drepturilor omului* ca fiind aplicabilă fiecărui stat semnatar în parte, şi este de datoria acestora de a garanta protecția lor: „Înaltele Părți Contractante recunosc oricărei persoane aflate sub jurisdicția lor drepturile şi libertățile definite în Titlul I al prezentei Convenții".

Ori, universalitatea protecției acestor drepturi fundamentale a fost rațiunea morală pe care s-a construit întreaga normă, rolul său fiind de a găsi o aplicare cât mai vastă şi nu limitată la normativul specific fiecărei națiuni. În sine Convenția exultă din aceleaşi idei morale, unificatoare, ca element definitoriu al civilizației noastre, definite de şi prin forma de guvernământ democratică.

În cazul *Bancovic şi alții* împotriva *Belgiei şi alții*[167], CEDO consideră că bombardamentul realizat de NATO în Serbia nu a reprezentat un exercițiu al jurisdicției, întrucât deciziile militare în spațiul extern nu fac obiectul acestei Convenții. Dreptul aplicabil este reprezentat de Convențiile de la Geneva, deci, „articolul 1 privind jurisdicția se aplică chestiunilor de ordin comun, iar din punct de vedere al dreptului internațional, competența jurisdicțională a statului este în primul rând teritorială". Deşi dreptul internațional nu exclude exercițiul puterii statale extrateritorial, baza unei astfel de jurisdicții (care include naționalitatea, steagul, relațiile diplomatice şi consulare) sunt acceptate ca regulă generală şi limitate de suveranitatea teritorială a celuilalt stat relevant. Deci, în opinia Curții, celelalte forme de jurisdicție, sunt excepționale.

---

[166] Convenția pentru apărarea Drepturilor Omului şi a Libertăților fundamentale, Roma, 1950 – Adunarea Generală a ONU.

[167] În cauză 6 cetățeni ai Republicii Federale Iugoslavia au depus acțiune în fața Curții de la Strasbourg împotriva 17 țări europene membre NATO, legat de misiunea de bombardare realizată pe 23.04.1999 care a avut ca obiectiv stația radio şi de televiziune sârbă din Belgrad şi care a dus la moartea a 16 persoane şi rănirea a altora. Reclamanții au arătat că prin operațiunea NATO le-a fost încălcat dreptul la viață, la libertatea de exprimare şi dreptul la o justă compensație.

Problema garantării respectului drepturilor la viață privată persoanelor, indiferent de cetățenie, a fost tratată de această manieră uniformizantă de ONU prin Rezoluția 68/169 pentru a creşte implicarea statelor în schimbarea politicilor naționale, datorită faptului că la nivel statal sunt diferențe de tratament pe criterii de teritorialitate şi de apartenența la cetățenia respectivă. Un caz important este reprezentat de cauza adusă în fața Curții Supreme, în 1990, *SUA* împotriva *Verdugo-Urquidez*[168], care în esență demonstrează că persoanele străine nu se bucură de aceleaşi drepturi şi garanții privind viața privată întrucât legea fundamentală a statului a fost gândită şi formulată având în vedere proprii cetățeni.

În materie de culegerea de informații din supravegherea electronică observăm că s-a preluat viziunea exprimată de Curte, aşadar, ținând cont de specificul special al serviciilor de informații, se consideră că jurisdicția extrateritorială exercitată nu încalcă prevederile dreptului internațional, acțiunile acestora fiind „o jurisdicție extraordinară".

Însă, sub aspectul *persoanelor vizate* se naşte discuția apartenenței la teritoriu, a naționalității, a oferirii unor garanții obligatorii cetățenilor proprii rezultat din aplicarea chiar a articolului 1 din Convenție. Un exemplu grăitor este reprezentat de felul în care se aplică Tratatul internațional privind supravegherea comunicațiilor (SIGINT), unde este clară distincția de tratament a persoanelor vizate, aceasta fiind realizată pe criteriul cetățeniei (între cetățeni, rezidenți permanenți şi non-cetățeni), întrucât legea națională fiecărui stat semnatar implică o serie de obligații față de proprii cetățeni.

Totuşi, practica rezultată din această interpretare nu trebuie să nască un tratament total diferit a cetățenilor de străini, aşa cum reține şi Curtea Supremă a Regatului Unit în *cauza Belmarsh*[169]. În 2005, reclamanții[170] au dus cauza în fața Curții de la Strasbourg, pentru ca în 2009 decizia Curții să fie că drepturile lor la libertate şi securitate au fost încălcate, fiindu-le acordate compensații pentru detenția nelegală.

---

[168] *Statele Unite* împotriva *Verdugo-Urquidez*, 1990 este un caz în care s-a decelat faptul că protecția prevăzută în cel de-al patrulea Amendament asupra vieții private nu se aplică în cazul percheziților şi sechestrelor realizate de agenții federali asupra bunurilor din străinătate deținute de persoane străine nerezidente. *Verdugo-Urquidez* era acuzat de trafic internațional de droguri. https://supreme.justia.com/cases/federal/us/494/259/ accesat la 20.01.2020.

[169] *A şi alții* împotriva *Secretarului de Stat pentru Afaceri Interne*, 2004 - cunoscut drept *cazul închisorii Belmarsh* - avea ca obiect detențiunea pe termen nelimitat a prizonierilor străini, fără a fi supuşi unei judecăți, prin efectul Legii Antiterorism, criminalitate şi securitate din 2001. Reclamanții au fost 9 străini care au fost amenințați cu deportarea fără judecată pentru că prezentau o amenințare la securitatea națională. Curtea Supremă (The House of Lords) a reținut că prevederile legale în baza cărora deținuții erau încarcerați erau incompatibile cu art. 5 din Convenția Europeană a Drepturilor Omului generând discriminarea persoanelor străine – totuşi, Secretarul de Stat nu a fost obligat să îi elibereze.

[170] Cei 9 reclamanți imigraseră în Regatul Unit, unde trăiau de ceva vreme, până când Secretarul de stat a decis să-i deporteze în lumina informațiilor că aceştia erau conectați într-un fel cu Osama bin Laden sau cu Al Qaeda.

Concluzia care transpare este că nu se pot face diferenţe în tratamentul persoanelor, exclusiv pe considerente de cetăţenie[171], însă contextul luptei antiteroriste şi a culegerii de informaţii din supraveghere, relevă faptul că nu există o legătură între apartenenţa la o cetăţenie anume şi comportamentul care ar putea reprezenta un pericol pentru securitatea naţională, având în vedere că atacul cu bombă din 07.07.2005 de la metroul din Londra a fost realizat de cetăţeni britanici, atacul armat din 05.11.2009 de la Fort Hood, Texas a fost realizat de Nidal Hasan, cetăţean american, maior în armata americană, atacul cu bombă din 15.04.2013 de la maratonul din Boston a fost realizat de fraţii Tsarnaev dintre care unul avea rezidenţa permanentă în SUA, iar celălalt este cetăţean american.

Având în vedere că dreptul la viaţă privată în era digitală a evoluat prin analogie cu operaţiunile fizice de căutare şi prin regres către procedurile existente analog, plecând, ori la sistemele naţionale, ori de la prevederile dreptului internaţional, ne aflăm în punctul de a concluziona că o astfel de interpretare generează rezultate îndoielnice, dacă încercăm să aplicăm această logică juridică şi culegerii de informaţii din supraveghere.

Spre exemplu, accesul fizic la un computer poate părea depăşit, dar trebuie notat că cele mai sensibile informaţii deţinute de entităţile statale şi private sunt stocate pe computere care nu sunt conectate la internet (în intranet) sau la alte reţele, chiar din necesitatea de a le proteja împotriva unor accesări neautorizate de la distanţă. Chiar şi de la distanţă, paşii procedurali pentru obţinerea accesului la dispozitivul respectiv trebuie să respecte rigorile procedurale pentru asigurarea legalităţii operaţiunii, respectiv, necesitatea ingerinţei şi proporţionalitatea măsurii.

Dacă urmărim logica morală a universalităţii drepturilor omului observăm şi diferenţa faţă de eficienţa practică, deoarece pe de-o parte aspirăm la *a urma logica morală a universalităţii*, să protejăm drepturile omului indiferent de locul în care se află acesta, plecând de la natura umană, pe de altă parte vom observa numeroasele dificultăţi practice şi politice în a atinge acest deziderat, precum şi faptul că natura umană nu este lipsită de obligaţii intrinseci, iar prin suprapunerea idealului universalităţii absolute realităţii practice, se poate distruge societatea în care trăim[172].

Efectele asupra societăţii a realizării culegerii de informaţii prin supravegherea electronică au fost întotdeauna accentuate în plan naţional, jurisprudenţa fiind axată pe procese purtate cu autorităţi judiciare sau servicii de informaţii faţă de

---

[171] *Gaygustus împotriva Austriei,* 1996, CEDO evidenţiază faptul că doar în situaţii extraordinare se pot considera legitime tratamentele diferenţiate asupra persoanelor fundamentat pe considerente de naţionalitate fără a încălca prevederile Convenţiei. „Fiecare din drepturile prevăzute în Convenţie trebuie protejate şi garantate, indiferent că persoana este cetăţean sau străin".

[172] Koskenniemi M., *From Apology to Utopia: The Structure of International Legal Argument*, Cambridge University Press, 2006, pp. 224-302.

respectarea procedurilor legale privind protecția vieții private şi a comunicațiilor private[173].

În cauza din 2018 *Ordre des barreaux francophones et germanophone* şi alții[174] ajunsă pe rolul Curții de Justiție a Uniunii Europene, la fel ca în cazul *Privacy International* şi alții[175], subiectul central îl reprezintă dacă se aplică Directiva privind viața privată şi comunicațiile electronice[176] la activitățile de securitate națională şi combatere a terorismului.

În primul caz, opinia formală a Avocatului General al Curții a fost prezentată, cauzele fiind în curs de soluționare, şi aceasta constă în faptul că Directiva se opune legislației care, similar celei belgiene, are ca obiect nu numai lupta împotriva terorismului şi infracțiunile grave, apărarea teritoriului, siguranța publică, dar şi investigarea, identificarea şi cercetarea unor infracțiuni mai puțin grave, şi în general, orice alte situații care vin sub incidența articolului 23 alin.(1) din Regulamentul 2016/69 (GDPR[177]). Motivul este că, în ciuda faptului că accesul la datele deținute face obiectul unor situații condiționate de lege, sarcina operaționalizării acțiunii generale şi nediscriminate de procesare, reținere a traficului de date şi a locațiilor revine operatorilor de servicii de comunicații, şi se aplică permanent şi continuu, ceea ce este contrar Convenției Europene a Drepturilor Omului.

În cel de-al doilea caz, chestiunea care necesită clarificare este dacă legislația națională este compatibilă cu Directiva 2002/58/EC atunci când impune unui operator de servicii de comunicații obligația de a transmite serviciilor de informații date din comunicații în masă, în urma unei colectări generale şi nediscriminatorii.

---

173 ECtHR Jurisprudence, Press Unit. Factsheet – Personal data protection 2017 https://www.privacyrules.com/privacy-global-expertise/ecthr-jurisprudence-0000447.html accesat în 06.01.2020.

174 Cauza CJUE C-520/18 (din 2018 în curs de soluționare) Belgia a cerut o hotărâre preliminară asupra legislației naționale care permite stocarea datelor personale de operatori în afara proceselor de prevenire a criminalității şi amenințărilor la securitatea națională, care sunt prevăzute ca **excepție** de Regulamentul GDPR din 2016 în art. 23 alin.(1).

175 Cauza CJUE C-623/17 (în curs de soluționare) în care Regatul Unit a cerut în 2017 o hotărâre preliminară privind culegerea generală a datelor private de la operatori de către serviciile de informații, în contextul în care procesul fusese deschis în 2015. În cursul procesului Privacy International argumentează că aceste mijoace şi metode nu sunt legale pentru că lipsesc garanțiile impuse de CJUE în decizia *Tele2/Watson*.

176 Directiva 2002/58/EC.

177 Regulamentul este aplicabil tuturor statelor membre ale Parlamentului European, iar unul din obiectivele cheie al GDPR este să se îndepărteze de climatul fragmentat al legislației naționale a celor 28 de state care puseseră în aplicare fosta Directivă 95/46/EC şi să ofere certitudinea legală pentru persoane şi companii în Uniunea Europeană. Chiar şi aşa, Regulamentul lasă la latitudinea legiuitorilor menținerea şi introducerea unor prevederi specifice adaptate aplicării anumitor reguli, de aceea atenția deosebită a Comisiei Europene(organismul de control) trebuie să se îndrepte în această direcție în care există şansele realizării unei fragmentări mai accentuate decât cea precedentă, fiind vorba de art. 6 alin. (2) şi (3) în care se exceptează acele prelucrări care survin din atribuțiile legale prevăzute în alte legi naționale.

Opinia formulată în cursul procedurilor din faţa CJUE a Avocatului General este că „în pofida prevederilor art. 4 din Tratatul Uniunii Europene – în baza căruia securitatea naţională este responsabilitatea exclusivă a fiecărui stat membru – Directiva privind viaţa privată şi comunicaţiilor este opusă legislaţiei Regatului Unit".

În esenţă, viziunea actuală reflectată de jurisprudenţa europeană este că **exceptarea de la obligaţiile privind păstrarea vieţii private, nu se extinde şi asupra operatorilor, întrucât aceştia nu deţin competenţe în securitatea naţională**, şi care fac parte din circuitul civil şi fiind subiecţi de drept comun, care trebuie să respecte prevederile legale privind drepturile persoanelor.

În 2019 Consiliul Uniunii Europene[178] transmis concluziile sale referitoare la îmbunătăţirea stocării datelor în scopul luptei împotriva criminalităţii, cu referire la prevederile din art. 25 alin.(1) din Regulamentul 2016/679, întrucât streaming-ul de date obţinut de la operatorii de comunicaţii reprezintă **un element important pentru organele de cercetare penală şi cele de urmărire penală în cursul investigaţiei activităţii infracţionale, precum terorismul în epoca digitală**. Aşadar, pentru a desfăşura investigaţii de succes autorităţile nu se pot baza doar pe datele deţinute de operatori în scop comercial. Acest scop comercial, în sine, nu reprezintă acea garanţie că datele sunt reţinute, şi dacă acele date sunt reţinute perioada pentru care sunt reţinute nu este predictibilă, şi nici nu există garanţia că operatorii respectivi stochează astfel de date necesare autorităţilor competente.

Consiliul reţine că din toate acestea s-a relevat necesitatea stabilirii unor **reguli noi**, transparente privind obligaţiile de stocare a datelor pentru operatorii de comunicaţii, care să îndeplinească şi nevoile operaţionale ale organelor de punere în aplicare a legii, dar care să ofere suficiente garanţii de respectare a drepturilor omului, aşa cum sunt prevăzute în Convenţie, mai exact dreptul la viaţă privată şi protecţia datelor cu caracter personal. De aceea este foarte important de observat Deciziile CJUE în cauzele *Digital Rights Ireland*[179] şi *TEle2/Watson*[180] în care s-a pronunţat doar supra tipurilor de date de trafic şi localizare, însă nu şi la datele privind abonaţii.

Făcând referire la concluziile Consiliului European din 23.06.2017[181] care puneau accent pe importanţa disponibilităţii datelor pentru eficienţa luptei împo-

---

[178] Opinia Consiliului Uniunii Europene privind *îmbunătăţirea reţinerii datelor în scopul luptei împotriva criminalităţii* nr. 7833/19 din 27.03.2019, prezentată în cadrul Comisiei de lucru DAPIX – Grupul de lucru privind schimbul de informaţii şi protecţia datelor.

[179] CJUE C-293/12 soluţionat în 2014.

[180] CJUE C-203/15 soluţionat în 2016.

[181] EUCO 8/17 - Consiliul European condamnă atacurile teroriste recente şi afirmă unitatea în lupta împotriva terorismului, urii şi extremismului violent, subliniind importanţa cooperării la nivelul Uniunii pentru creşterea securităţii interne prin măsuri eficiente împotriva radicalizării on-line, va coordona activităţile de prevenire şi contracarare a extremismului violent, va opri finanţarea terorismului, va facilita schimbul de informaţii rapid şi eficient între autorităţile de aplicare a legii,

triva criminalității grave şi a terorismului, Consiliul Uniunii Europene subliniază că existența unor diferite norme naționale pentru stocarea de date ar fi contraproductivă pentru cooperarea şi schimbul de informații dintre autoritățile competente, sens în care concluziile Consiliului European din 18.10.2018 se adresează statelor membre să găsească măsuri comune pentru a *acorda autorităților competente instrumente adecvate pentru a putea face față noilor provocări apărute din dezvoltarea tehnologiei şi a schimbării peisajului amenințărilor la securitatea națională* chiar prin punerea echipamentelor în comun, parteneriate sporite cu sectorul privat, cooperarea inter-agenții şi o mai bună accesare a datelor[182].

În contextul jurisprudenței CJUE în materie de reținerea datelor de către operatori pentru a le ajuta pe autorități să documenteze cazurile de terorism şi criminalitate gravă, Consiliul solicită o analiză asupra opțiunilor existente pentru asigurarea accesibilității la datele necesare instituțiilor statului, menționând raportul Comisiei speciale asupra terorismului din cadrul Parlamentului European în care se subliniază nevoia unui cadru legal privind reținerea datelor adecvată liniei de gândire impuse de jurisprudența CJUE. Chiar dacă regulile din actuala Directivă 2002/58/EC[183], alături de structura legislativă reformată a Uniunii Europene, mai ales GDPR şi Directiva privind organele de aplicare a legii, alături de negocierile purtate cu privire la propunerea Comisiei Europene pentru o nouă *Directivă asupra vieții private şi comunicațiilor digitale* sunt **esențiale pentru *scopul* stocării datelor personale.**

De asemenea, Consiliul Uniunii Europene[184], în pregătirea evaluării asupra modalității de implementare a GDPR realizate de Comisia Europeană, reține că

---

incluzând şi partenerii de încredere externi şi se va îmbunătăți interoperabilitatea dintre bazele de date. Industria privată are şi ea responsabilitatea de a ajuta combaterea terorismului şi infracționalității digitale prin implementarea unor instrumente de detecție şi eliminare automată a conținutului care incită la acte de terorism. (ideea a fost implementată de giganții media YouTube, Facebook aşa cum se analizează în articolul *YouTube şi combaterea radicalizării* de Lascateu C., Medeşan A, Revista Intelligence nr. 35, 2017, pp. 86-89). Consiliul European consideră că **un acces eficient la probe electronice este esențial în combaterea infracțiunilor grave şi a terorismului, aşadar disponibilitatea accesului la aceste date trebuie asigurată.**

[182] EUCO 13/18 – Consiliul European concluzionează la 18.10.2018 că măsurile de prevenire a migrației ilegale şi a traficului de persoane ca forme de criminalitate trebuie să beneficieze de monitorizarea comunicațiilor electronice a traficanților pentru a fi aduşi în fața justiției, scop în care, cu sprijinul Comisiei Europene îşi propune să dezvolte un set de măsuri comprehensive şi operaționale care să asigure grupului de lucru creat în cadrul Centrului european de trafic de carne vie din cadrul Europol, mijloacele necesare. Totodată, Consiliul European subliniază necesitatea creşterii capacității de prevenire şi răspuns eficient la radicalizare şi terorism, cu deplina respectare a drepturilor omului. **Trebuie găsite soluții pentru asigurarea unei rapide şi eficiente accesări transfrontaliere a probelor digitale ca să putem lupta eficient împotriva terorismului şi a altor infracțiuni grave, atât în cadrul Uniunii Europene, cât şi în plan internațional.**

[183] Privind procesarea datelor personale şi protecția vieții private în sectorul de comunicații electronice, modificată prin Directiva 2009/1369/EC.

[184] În 15.10.2019 în pregătirea pentru opinia transmisă Comisiei Europene asupra aplicării GDPR nr. 12991/19.

scopul acestui Regulament este să realizeze o poziție puternică şi coerentă în abordarea structurii de protecție a datelor cu caracter personal, printr-o implementare eficientă, având două obiective: să protejeze drepturile şi libertățile fundamentale ale omului, şi în particular dreptul oamenilor de a avea protecția datelor private, şi garantarea fluxului liber a datelor şi dezvoltarea continuă a economiei digitale în toate piețele interne. Deopotrivă, Consiliul notează faptul că fenomene precum **noile tehnologii care se dezvoltă reprezintă noi provocări pentru protecția datelor personale**, acestea fiind legate de domeniile big dat şi discriminare, folosirea inteligenței artificiale şi a tehnologiei bazate pe blockchain, iar unul din punctele care ar trebui să fie în raportul Comisiei Europene este dacă GDPR răspunde acestor provocări. De asemenea, Consiliul subliniază **necesitatea armonizării întregii legislații europene** făcând trimitere la necesitatea congruenței GDPR cu Directiva 2016/680[185] privind protecția persoanelor private privind prelucrarea datelor de către autorități în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor şi privind libera circulației a acestor date. În esență, Consiliul susține că **protecția datelor ar trebui avută în vedere atunci când sunt inițiate politici publice care afectează procesarea acestor date.**

Punând în balanță pe de-o parte abordarea şi investiția politică în supravegherea prin tehnologie şi pe de altă parte formalismul procedural impus de conformitatea legală, se întrevede totuşi o zonă în care se lasă loc continuării şi dezvoltării programelor de culegere de informații prin astfel proceduri. Aceasta se relevă şi din analiza jurisprudenței ce pune accent pe ideologia drepturilor fundamentale ale omului şi mai puțin pe înțelegerea practică a ceea ce presupune securitatea datelor personale în era digitală.

Deopotrivă se poate observa şi lipsa punerii în aceleiaşi categorie de importanță a protecției datelor private cu cea a securității cibernetice, deoarece dacă nu deții securitatea sistemelor şi mijloacelor de comunicații, nu asiguri o protecție a datelor personale, în timp ce accentul este pus pe rigorile procedurale privind răspunderea legală asupra măsurilor de culegere de informații, sub aspectul proporționalității, obiectivității şi necesității într-un stat de drept, fără a se menționa procedurile fizice de protejare a datelor, măsuri circumscrise domeniului tehnologic al securității cibernetice privind datele private.

[185] Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor şi privind libera circulație a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului

4. CULEGEREA DE INFORMAȚII DIGITALE - PERSPECTIVA DEONTOLOGICĂ

Culegerea de informații de securitate națională este una din zonele principale de decizie într-un stat, pe care guvernarea nu este dispusă să o supună dezbaterii publice sau controlului judiciar, sau mai mult, controlului sau supravegherii internaționale, după cum reține Comisia de la Veneția[186] în cea de-a 71-a Sesiune Plenară[187].

În contextul evoluției dreptului umanitar internațional, conflictele contemporane au ridicat noi provocări la normativul internațional existent, iar noile standarde rezultate din practica judiciară națională şi din legiferare îşi pun amprenta asupra felului în care sunt gestionate de curțile internaționale problematicile ridicate privind dreptul la viață privată. Aceeaşi concluzie privind evoluția dreptului internațional se referă şi la practicile de culegere de informații de către actori statali, mai ales în privința supravegherii comunicațiilor globale.

Discrepanța care apare este între cadrul legal, teoretic, şi modalitatea de implementare în practică, adaptarea tehnologică la cadrul legal. Deopotrivă, este importantă şi clarificarea juridică a limitelor existente a măsurilor de culegere de informații, raportat la limitele exercitării suveranității statului.

Aşa cum statuează Comentariul 16 al Consiliul Drepturilor Omului[188], culegerea de informații din mediul personal de către autoritățile publice „trebuie stabilită prin lege". În principal, *legalitatea* presupune, pe de-o parte, cunoaşterea de către persoanele supuse supravegherii electronice, pe de altă parte, cunoaşterea autorităților sub a căror competențe legale se realizează respectiva culegere de informații.

Etica şi dreptul nu sunt tematici identice, în ciuda tendinței generale de a le unifica, sau chiar în mod greşit a considera că Legea este fundamentul de la care pleacă normele comportamentului uman. Chiar în mod contrar, atunci când Legea nu vorbeşte despre tipuri noi de conflicte în mod concret, este necesar să recurgem la etică pentru a clarifica ipostazele în care ne aflăm: să distingem spre exemplu, care sunt principiile fundamentale de drept şi jurisprudența relevantă ce poate fi invocată pentru a ne ghida în desluşirea unei controverse precum apariția divergențelor între state în spațiul cibernetic. Problema care se pune este dacă normele existente şi principiile morale convenționale se aplică spațiului cibernetic, şi dacă

---

[186] Denumită oficial: ***Comisia Europeană pentru Democrație prin Drept***, este organ consultativ al **Consiliului Europei** alcătuit din experți independenți în domeniul dreptului constituțional, înființată în 1990, după căderea Zidului Berlinului.

[187] Comisia de la Veneția *The Report on the Democratic oversight of the Security Services* adoptat la cea de-a 71-a sesiune Plenară, Veneția, 1-2.06.2007, par. 81.

[188] Comitetul pentru Drepturile Omului din cadrul Națiunilor Unite, *Comentariul 16: articolul 17 (dreptul la viață privată) dreptul la respectarea vieții private, a familiei, a căminului şi a corespondenței şi protecția onoarei şi a reputației* adoptată în cea de-a 32-a sesiune a Comitetului pentru drepturile omului, 08.04.1988.

acestea sunt cele mai bune şi eficiente mijloace de protejare a păcii şi securității în condițiile în care statele îşi construiesc constant capabilități cibernetice[189].

4.1 Ecosistemul procedural privind culegerea de date private digitale

Ca moment determinant pentru era informațiilor digitale de securitate națională, atât politic cât şi normativ, se remarcă dezvăluirile din 2013 realizate de Edward Snowden despre întinderea programelor de culegere de informații prin supraveghere tehnică gestionate de Statele Unite ale Americii şi partenerii strategici, în mare parte dinte acestea fiind vorba de Regatul Unit, au provocat pe lângă interesul public ridicat asupra caracterului aparent *nelimitat* al măsurilor implementate de culegere de informații[190], şi o dilemă juridică asupra competențelor legale pentru desfăşurarea unor astfel de tehnici de documentare în scopul apărării intereselor de securitate națională.

Problema teritorialității puterii executive, fiind legată strict de apărarea intereselor naționale, în cazul acestor mijloace de culegere de informații, acesta este extrapolată în plan universal, supranațional, păstrându-şi scopul inițial de a obține primordialitatea obiectivelor, numai că limitele exercitării acestor măsuri sunt creionate de tratate internaționale, de exercitarea puterii statale în plan strategic. În această paradigmă, ne raportăm şi la protecția drepturilor omului, care survine din dorința interstatală de a garanta o interpretare comună, universală a normelor garanții privind umanitatea, chiar dacă practica poate fi diferită de la stat la stat. Normativul moral din care au izvorât tratatele de protejare a drepturilor omului fiind factorul unificator al comunității internaționale, dar şi obligatorie ca normă ratificată în dreptul intern. Din aceste motive, dezvăluirile sus-menționate pun în discuție publică „jurisdicția", consecințele resimțite fiind de ordin politic.

Acest rezultat este relevat din faptul că prin aplicarea tratatului multilateral adoptat de Adunarea Generală a Națiunilor Unite din 16 decembrie 1966 privind Convenția internațională a drepturilor civile şi politice ale omului prin sancțiunile Comisiei Drepturilor Omului, sau cele ale Curții Europene ale Dreptului Omului de la Strasbourg asupra statelor, acestea sunt diferite, şi o calificare mai exactă ar fi că se încadrează în zona politică, scopul fiind ralierea politicilor publice la dezideratul moral cuprins în normele internaționale.

Un exemplu este reprezentat de cazul care a făcut obiectul Curții Internaționale de Arbitraj Permanent de la Haga[191] dintre Australia şi Timorul de

---

[189] Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare*, Oxford University Press, 2017, pp. 40-41.

[190] Milanovic M. *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, vol.56, nr.1, 2015, pp. 81- 146.

[191] În contextul în care în 2002 Australia s-a retras din Convenția Națiunilor Unite a dreptului mărilor (UNCLOS) care ar face o decizie a Curții Internaționale de Justiție de la Haga obligatorie şi de strictă interpretare în materie de dispute teritoriale, două luni mai târziu Timorul de Est devine

Est[192], în contextul în care țările erau cosemnatare a unui Tratat de exploatare a rezervelor de petrol din Marea Timorului. În cursul procesului de arbitraj membrii ai Serviciul Secret de Informații al Australiei (ASIS)[193] s-au prezentat ca fiind muncitori în construcții şi au instalat tehnică de interceptare în pereții celor mai înalți demnitari ai țării vecine. Acuzația adusă Australiei în fața Curții Internaționale de Justiție, a fost a fost că a obținut şi a păstrat date electronice şi documente încălcând suveranitatea Timorului de Est, privind arbitrajul ce avea loc[194]. Scopul operațiunii a fost obținerea de informații vitale pentru negocierea ostilă privind rezervele de petrol şi gaze din strâmtoarea Timorului dintre cele două state dusă în fața Curții de Arbitraj, fapt confirmat şi de ofițerul de informații ASIS care a condus operațiunea de interceptare din 2004, a declarat în 2012 că prin aceste mijloace Guvernul Australian a avut acces la informații secrete de cel mai înalt nivel discutate de guvernul Timorului de Est care au profitat strategiei de negociere[195].

Dezvăluirea operațiunii de interceptare[196] a Guvernului din Timorul de Est a fost decisă de Inspectoratul General al Activității de Informații şi Securitate al Australiei[197] organ de supervizare a activităților serviciilor de informații australiene.

Acest caz arată că *de lege lata*, aplicarea tehnicilor de spionaj pe timp de pace este strict interzisă de dreptul internațional public, atrăgând sancțiuni statului care încalcă aceste principii general valabile, însă, trebuie avut în vedere că activitatea de culegere de informații externe este o expresie a suveranității, deci, un drept al statului care asigură, corolar, fundamentul independenței. O astfel de viziune ce

---

independent față de Indonezia, aşadar, în 2004 încep negocierile privind recunoaşterea teritorială dintre Timorul de Est şi Australia. În acelaşi timp a debutat operațiunea serviciului de informații externe al Australiei pentru a obține date şi informații privind negocierile tratatului şi a fi folosite în avantaj. Cu 18 luni înaintea instalării tehnicii de interceptare avusese loc exploziile din Bali, insulă aflată în sudul Asiei. (*East Timor spying scandal: Tony Abbott defends ASIO raids on lawyer Bernard Collaery's offices,* ABC, 04.12.2013 https://www.abc.net.au/news/2013-12-04/asio-arrests-key-witness-in-east-timor-spying-scandal/5132954 accesat la 20.12.2019).

[192] Curtea Internațională de Arbitraj Permanent de la Haga, *Timor Leste împotriva Australiei*, 2015-42, Curtea Internațională de Justiție 2013-16.

[193] Serviciul de informații externe al Australiei.

[194] Măsuri impuse de Curtea Internațională de Justiție în cazul *Timor Leste* împotriva *Australiei* https://www.icj-cij.org/en/case/156/provisional-measures.

[195] Wilkinson M, Cronau P. *Drawing the Line,* ABC, 24.03.2014, https://www.abc.net.au/4corners/drawing-the-line/5328634 accesat la 20.12.2019.

[196] Keane B. *Open and shut: ASIS crime and the Labor Liberal cover-up,* Crikey, 12.06.2015.

[197] Instituție înființată în 1986, independentă funcțional, dar care face parte din portofoliul primului ministru, competentă cu auditarea activităților a şase servicii de informații australiene care formează comunitatea australiană de informații. Această instituție este o parte importantă din sistemul de responsabilizare din cadrul guvernului australian, controlând legalitatea activităților serviciilor de informații, respectarea politicilor guvernamentale în domeniul securității naționale şi respectarea drepturilor omului.

transpare ca interpretare într-o notă imperialistă referitor la activitatea de informații externe este analizată de A. Lubin care concluzionează că această activitate este de fapt o „doctrină a abuzului de drept centrată pe folosirea şi / sau *abuzul de discreție*[198] de către un subiect de drept internațional”[199].

Ideea principală urmărită de Lubin este că activitatea de informații este încadrată juridic ca *drept la legitimă apărare a unui subiect de drept*, acesta fiind statul. Această abordare juridică conceptualizează sensul strategiilor urmate de serviciile de informații în folosul securității, şi totuşi, această abordare implică o serie de limitări născute din subiectivismul regulilor aplicabile în acest domeniu.

Dacă ne raportăm exclusiv la această viziune legată de *legitimă apărare*, spectrul activității de informații s-ar rezuma la realizarea activităților specifice, cu rol preemptiv, exclusiv în cazul actorilor cunoscuți, discurs care duce la concluzia că statul are dreptul să *supravegheze global* în interesul securității, aserțiune care necesită o calificare a limitelor şi scopului acestor tipuri de activități, ținând cont de îndatorirea fundamentală de protejare a drepturilor omului de către stat. Aceasta este diferența dintre exercițiul de culegere de informații prin supraveghere în masă, în mod legitim şi proporțional, sau desfăşurarea acestei activități în mod abuziv.

Un alt exemplu ar fi supravegherea realizată de către Serviciul de informații britanic GCHQ[200] în perioada 2009-2010 asupra şefului[201] Organizației Mondiale a liberului Schimb[202] şi a unor conducători africani[203], dezvăluire realizată de Edward Snowden furnizând jurnaliştilor informații extrase neautorizat din serverele NSA. Comunicatul de presă al GCHQ legat de aceste date publicate includea faptul că „serviciul desfăşoară numai activități autorizate, necesare şi

---

198 Terminologie introdusă în dreptul international public de G.D.S. Taylor în lucrarea *The Content of the Rule Against Abuse of Rights in International Law*, 46 Brit 46 Brit. Y. B. Int'l L. 323, 1972-1973, în care argumentează, plecând de la principiul de drept internațional potrivit căruia *nicio persoană nu poate abuza de drepturile sale*, şi preluând argumentele lui Sir H. Lauterpacht din *The Function of Law in the International Community, Oxford* 1933, acesta defineşte ***abuzul de drept*** ca un instrument general de a îndrepta toate eforturile circumscrise suveranității statului către influențarea dreptului internațional, având în vedere că dreptul internațional este un drept al tratatelor, cutumiar. Dacă se pleacă de la premisa că un stat suveran dictează altui stat o anumită conduită, este necesară o calificare imediată a faptei. Un stat nu poate acționa pe teritoriul altui stat fără permisiunea acestuia pe timp de pace (Cazul *Lotus*, CIJ, 1927), dar există limite de expresie asupra drepturilor fiecărui stat de a-şi exprima suveranitatea.

199 Lubin A. *Espionage as a Sovereign Right under International Law and its Limits*, ILSA, vol. 24, nr. 3, 2016, pp. 22-28.

200 Government Communications Headquarters GCHQ, echivalentul National Security Agency NSA.

201 Pascal Lamy şeful World Trade Organisation WTO, membru al Partidului Socialist din Franța.

202 Gallagher R., *Extensive British Spying throughout Africa revealed in Le Monde*. The Intercept 2016, https://archive.is/V6NEM accesat la 14.12.2019.

203 Piel S, Tilouine J. *British spying: tentacles reach across Africa's heads of states and business leaders*, Le Monde, 2016, https://archive.is/UxcMW accesat la 14.12.2019.

proporționate, care sunt în deplină concordanță cu prevederile Convenției drepturilor omului".

Având în vedere cadrul legal internațional reprezentat de protecția drepturilor fundamentale ale omului prin tratate de importanță majoră[204] la care au aderat state care dețin înaltă tehnologie de supraveghere în masă, precum Germania, Franța şi Rusia, interesul nostru se axează pe faptul că viața privată[205] este protejată de aceste acte internaționale. Dilema ce apare în situația supravegherii, este dacă prevederile respective se aplică şi supravegherii extrateritoriale, adică, dacă se aplică culegerii de informații.

În cauza *Big Brother Watch* contra *Regatului Unit al Marii Britanii*[206], Curtea Europeană a Drepturilor omului a decis că supravegherea în masă **încalcă drepturile omului** prin lipsa de incorporare a unor măsuri precise de protejare a vieții private şi a unei forme de control extern asupra tipurilor de măsuri întreprinse, însă **acestea nu au încălcat dreptul internațional**. Decizia Curții se bazează pe respectul vieții de familie şi a dreptului la liberă exprimare față de adunarea masivă de date folosită asupra cetățenilor britanici de serviciul de informații britanic. Cazul a adus în discuție şi formele de cooperare şi schimbul de informații dintre serviciile de informații, aspecte care au fost considerate conforme prevederilor internaționale angajate de statele implicate.

Curtea reține, totodată că natura juridică a culegerii de informații din mediul comunicațiilor de pe internet prin intermediul accesului la comunicații cu sprijinul operatorilor (programele PRISM şi Upstream) are susținere legală în normele naționale ale Regatului Unit şi păstrează echilibrul puterii exercitate de stat şi cetățeni, din perspectiva proporționalității măsurilor desfăşurate, în sensul prevederilor Convenției europene a drepturilor omului.

Mai mult, Curtea are în vedere că supravegherea în masă chiar dacă nu se dovedeşte a fi ilegală, este susceptibilă de a putea naşte abuzuri, dat fiind accesul fizic la rețeaua de fibră optică (programul TEMPORA) şi lipsa unei ținte precise a

---

[204] Pactul internațional cu privire la drepturile civile şi politice ale omului, 1966 (intrat în vigoare în 1967) – Consiliul Europei şi Convenția pentru apărarea Drepturilor Omului şi a Libertăților Fundamentale (Convenția Europeană a Drepturilor Omului) 1950 (intrată în vigoare în 1953) - Adunarea generală a Consiliului Organizației Națiunilor Unite.

[205] Art.12 din Declarația universală a drepturilor omului, 1948: *„Nimeni nu va fi supus la imixtiuni arbitrare în viața sa personală, în familia sa, în domiciliul lui sau în corespondența sa, nici la atingeri aduse onoarei şi reputației sale. Orice persoană are dreptul la protecția legii împotriva unor asemenea imixtiuni sau atingeri.*", respectiv art. 17 din Pactul internațional privind drepturile civile şi politice ale omului, 1966 *„Nimeni nu va putea fi supus vreunor imixtiuni arbitrare sau ilegale în viața particulară, în familia, domiciliul sau corespondența sa, nici la atingeri ilegale aduse onoarei şi reputației sale. Orice persoană are drept la protecția legii împotriva unor asemenea imixtiuni sau atingeri".*

[206] La **13.09.2018** Curtea de la Strasbourg a pus în discuție 3 tipuri de supraveghere tehnică realizate de serviciul de informații britanic GCHQ: interceptarea în masă a comunicațiilor în cadrul programului TEMPORA, cooperarea informativă cu NSA în cadrul programelor americane PRISM şi Upstream şi obținerea comunicațiilor de la operatori.

culegerii de informații. O astfel de supraveghere nu garantează respectarea dreptului la viață privată în sensul statuat de Convenție, întrucât supravegherea ar trebui să poată fi accesată de persoana vizată şi să aibă rezultate previzibile.

Deci, Curtea s-a raportat la principiile predictibilității şi necesității într-o societate democratică a activităților întreprinse de instituțiile statului față de persoane private, realizând analiza individuală a următorilor paşi identificați ca fiind importanți pentru soluționarea conflictului:

Prezintă valoare pentru interesele informative	1. Interceptarea unui procent mic al utilizatorilor de internet selecționați ca fiind cei mai probabili să realizeze comunicații externe
	2. Filtrarea şi eliminarea automată (aproape în timp-real) unui procent semnificativ al informațiilor interceptate
3. Formarea unei baze de date organizată pe multiple criterii de regăsire	
4. Reținerea acelor date care corespund criteriilor selectate	
5. Eliminarea datelor care nu răspund criteriilor de selecție definite	
6. Examinarea materialului reținut de către analistul de informații	

În clarificarea respectării principiilor predictibilității şi a necesității fiecărei etape, Curtea a aplicat un set de condiții minime:

- Natura faptelor care pot duce la obținerea unei autorizații de interceptare,
- Definiția categoriilor de persoane susceptibile de a avea comunicațiile interceptate,
- Durata perioadei de interceptare,
- Procedura urmată pentru examinarea, folosirea şi stocarea datelor obținute,
- Măsurile de protecție necesare a fi implementate pentru transmiterea datelor către terți,
- Circumstanțele în care datele interceptate pot şi trebuie şterse sau distruse.

Aşadar, Curtea a arătat că este lipsită de predictibilitate supravegherea în masă, față de tipul de persoane vizate de program, iar procesul de selecție a datelor de valoare informativă, realizarea categoriilor de informații după care se pot implementa criterii de regăsire pentru a decide care date vor fi reținute, precum şi criteriile de selecție a datelor ce vor fi examinate de analişti sunt contrare prevederilor privind dreptul la viață privată, fiind realizate fără suficiente instrumente de protecție împotriva potențialelor abuzuri, prezentând un grad mare de subiectivism, dar şi o lipsă de transparență față de principiile concrete ale funcționării bazei de date realizate.

Deopotrivă Curtea statuează faptul că metadatele[207] impun alte proceduri de protecție privind viața privată față de datele extrase din comunicații, şi că nu toate

[207] *Metadatele* sunt date care oferă informații despre alte date, acestea fiind de mai multe tipuri: metadate descriptive, structurale, administrative, de referință şi statistice. (Zeng M. *Metadata Types and functions* NISO 07.10.2016).

metadatele impun acelaşi nivel de protecţie, însă, datele conexe comunicaţiilor urmărite de autorităţi nerestricţionat precum geolocaţia[208], istoricul căutărilor, datele de trafic, rerutarea telecomunicaţiilor digitale, informaţiile despre caracteristicile echipamentului, sunt legate de viaţa privată a persoanelor.

Faţă de proporţionalitate, Curtea consideră că programele de supraveghere sunt justificate de climatul internaţional sociopolitic, făcând trimitere la raportul Comisiei de la Veneţia care a concluzionat că informaţiile obţinute din supravegherea în masă reprezintă „o capabilitate esenţială mai întâi datorită faptului că teroriştii, criminalii şi serviciile de informaţii ostile au devenit sofisticate în eludarea detecţiei prin mijloace tradiţionale, dar şi datorită naturii globale a internetului care presupune ca traseul unei anumite comunicaţii să fie impredictibil."

Ca impact asupra legislaţiei naţionale, cazul a dus la modificarea normelor legale britanice prin care s-au întărit cheile de control de legalitate şi proporţionalitate, dar şi procedurile de supraveghere, chiar dacă decizia Curţii de la Strasbourg nu a criticat direct cadrul legal existent, ci doar politica naţională referitoare la supraveghere. Mai mult s-a înfiinţat o formă de control extern, independent a activităţii de culegere de informaţi din supravegherea în masă, în forma Comisarului competenţelor de investigare (Investigatory Powers Commissioner[209]).

Deopotrivă, respectarea corespunzătoare a drepturilor omului a fost pusă în discuţie, la nivel statal, încă din 2013, în lumina culegerii de informaţii asupra conducătorilor Braziliei şi a Germaniei dezvăluite în presă potrivit cărora guvernul american avusese astfel de măsuri, drept urmare cele două state au depus un proiect de rezoluţie către Comitetul al treilea al Adunării Generale a Naţiunilor Unite intitulată „Dreptul la viaţă privată în era digitală"[210]. Ceea ce este interesant este că aliaţii din tratatul celor cinci parteneri[211] (Australia, Canada, Noua Zeelandă, Regatul Unit şi Statele Unite ale Americii) au argumentat că protecţia

[208] *Geolocaţia* este identificarea ori estimarea poziţionării geografice a unui obiect electronic precum o sursă radar, un telefon mobil, un terminal conectat la internet. O formă simplistă de geolocaţie implică generarea unui set de coordonate geografice şi este legată direct de sistemele de poziţionare, însă utilitatea sa este crescută de folosirea acestor coordonate pentru a determina locaţia în spaţiul geografic, precum o adresă stradală. (Ionescu D. *Geolocation 101: How It Works, the Apps and Your Privacy*, PCWorld, 29.03.2010).

[209] Instituţie înfiinţată în 2016, în Regatul Unit, prin Legea competenţelor de investigare (Investigatory Powers Act).

[210] Harris S, Hudson J., Lynch C. *Germany, Brazil Turn to UN to Restrain American Spies*, Foreign Policy, 25.10.2013.

[211] „Five Eyes" este o alianţă a serviciilor de informaţii din Australia, Canada, Noua Zeelandă, Regatul Unit şi Statele Unite ale Americii, state semnatare ale acordului multilateral de cooperare în domeniul SIGINT din 1941. Originar, tratatul a survenit în urma celui de-Al Doilea Război Mondial, pentru ca în timpul Războiului Rece programul de supraveghere ECHELON să monitorizeze Uniunea Sovietică şi Blocul Estic, însă acum este folosit pentru monitorizarea comunicaţiilor globale.(Asser M. *Echelon: Big Brother without a cause?* BBC, 06.06.2000) Ca parte a eforturilor luptei antiteroriste, din 2001, aliaţii şi-au sporit capabilităţile de supraveghere mai ales pe internet.

vieții private reprezintă o chestiune teritorială, națională, ce nu se transpune extrateritorial, nefiind sancționată de dreptul internațional. Totuşi, rezoluția a fost adoptată fără un singur vot de Adunarea Generală a Organizației Națiunilor Unite la 21.01.2014, făcând legătura directă cu prevederile art. 12[212] din Declarația Universală a Drepturilor Omului şi art. 17[213] din Pactul internațional privind drepturile civile şi politice.

De asemenea, referitor la transmiterea de date private transatlantic, inițial, principiile[214] se refereau la activitatea comercială şi a au fost dezvoltate între 1998 şi 2000 cu scopul de a preveni organizațiile private din SUA şi UE care stochează datele utilizatorilor de a le dezvălui accidental. Acestea au fost dizolvate de Curtea de Justiție Europeană în 2015[215], în urma demersului unui utilizator împotriva companiei Facebook, care reclama faptul că Facebook nu respectă reglementările europene privind viața privată şi transferă datele personale către NSA, prin participarea la programul PRISM.

În 2016 Comisia Europeană şi SUA au încheiat un nou cadru legal de transfer a fluxurilor de date cunoscut ca „Protecția datelor private UE-SUA[216]" care acoperă partea comercială a acestor transferuri. Totuşi, în 2017 Preşedintele SUA a adoptat un ordin executiv numit „Creşterea siguranței populației" care prevede că protecția vieții private garantate de SUA nu se extinde asupra străinilor sau non-rezidenților, care a fost contestat la Curtea Supremă ca fiind neconstituțional, aşadar în 21.11.2017 aplicarea acelei secțiuni privind viața privată a fost

---

[212] Art.12 din Declarația universală a drepturilor omului, 1948, *Nimeni nu va fi supus la imixtiuni arbitrare în viața sa personală, în familia sa, în domiciliul lui sau în corespondența sa, nici la atingeri aduse onoarei şi reputației sale. Orice persoană are dreptul la protecția legii împotriva unor asemenea imixtiuni sau atingeri;*

[213] Art. 17 din Pactul internațional privind drepturile civile şi politice, 1966, *Nimeni nu va putea fi supus vreunor imixtiuni arbitrare sau ilegale în viața particulară, în familia, domiciliul sau corespondența sa, nici la atingeri ilegale aduse onoarei şi reputației sale. Orice persoană are drept la protecția legii împotriva unor asemenea imixtiuni sau atingeri.*

[214] *The International Safe Harbor Privacy Principles*, sau *Safe Harbour Privacy Principles* conțineau 7 principii care erau în concordanță cu Directiva europeană privind datele cu caracter personal şi principiile elvețiene şi au fost elaborate de Departamentul Federal de Comerț al SUA. Prin Decizia Comisiei Europene 2000/520/EC prin care se constată conformitatea principiilor cu Directiva 95/46/EC.

[215] CJUE C-362/14 *Schrems* contra *Irlandei*, reclamantul fiind student la drept şi pentru un semestru studia într-o universitate americană, s-a hotărât să scrie o lucrare despre lipsa de cunoaştere a Facebook față de legislația europeană privind viața privată în urma unei prelegeri ținute de avocatul companiei în campusul universitar. În acest context a realizat o cerere pe baza dreptului european de a-i fi comunicate toate datele private stocate de companie, primind un CD cu 1200 de pagini de date, care în 2011 au dus la plângeri împotriva companiei la autoritatea națională irlandeză de protecție a datelor personale. Acesta a arătat că setul de principii Safe Harbour nu i-au oferit protecția datelor private.

[216] În *en. „the EU-US Privacy Shield"* din 08.07.2016 nu cuprinde referiri la ştergerea datelor, culegerea masivă de date, şi mecanismul Ombudsperson.

suspendată. Comisia Europeană a admis faptul că *Legea vieții private a SUA*[217] nu oferea protecția datelor private europenilor, aşa că a negociat şi instrumentul denumit „Acordul umbrelă UE-SUA[218]" intrat în vigoare în 2017, iar Congresul American a adoptat Legea regresului în justiție în 2016, care extinde beneficiile *Legii vieții private* şi către europeni.

Ceea ce este interesant este că norma juridică îmbracă forma intereselor politice antagoniste, în care corporații deopotrivă cu guverne pot desfăşura culegerea de informații private în limitele impuse de dreptul la viață privată, deoarece preocuparea a fiecărui stat este de a-şi proteja cetățenii în intimitatea lor, în acelaşi timp menținând demersurile politice de a culege informații cu ajutorul tehnologiei, deoarece, în fond, securitatea datelor şi culegerea de de informații în masă sunt concepte opuse.

4.2. Elementele deontologiei în culegerea de informații private în spațiul virtual - extrateritorialitatea

Ca fenomen, creşterea interesului pentru reglementarea spațiului cibernetic, respectiv a *extrateritorialității*[219] *virtuale* ca expresie a puterii statale şi expresie a competențelor legitime de a acționa în acest spațiu se arată a fi un demers polarizat de statele care deja dețin capabilități în spațiul cibernetic, a căror interes rezidă în aserțiunea autorității, a controlului asupra spațiului cibernetic. În această problematică, punctul de vedere moral este mai degrabă structural decât psihologic, aşa cum se dovedeşte a fi şi dreptul internațional înaintea apariției internetului[220], ca fiind axat pe stat-națiune, dependent de paradigme.

---

[217] În *en. „The US Privacy Act"* din 1974 legea are ca scop protejarea vieții private a persoanelor față de folosirea neadecvată a datelor federale şi pentru a oferi persoanelor acces la acele date referitoare la persoana lor deținute de agențiile federale.

[218] Acordul UE-SUA privind protecția datelor intrat în vigoare în urma Deciziei UE 2016/920 de semnare a acordului privind protecția datelor private în legătură cu prevenirea investigarea, identificarea şi cercetarea infracțiunilor şi a acordurilor asupra standardelor de protecție a transferurilor de date personale între autoritățile de aplicare a legii între UE şi SUA.

[219] Este **regimul special specific dreptului internațional** aplicabil în special persoanelor, dar şi bunurilor imobile şi se referă la privilegii şi imunitate de jurisdicție izvorâte din tratate, acordate pe baza reciprocității (şefii de stat, ambasadorii, bazele militare ale statelor străine, locațiile organizațiilor internaționale precum cea a ONU şi navele în apele internaționale). În plan național vorbim de **extrateritorialitatea legii penale** – art. 9 Cod penal „Legea penală română se aplică infracțiunilor săvârşite în afara teritoriului țării de către un cetățean român sau de o persoană juridică română, *dacă pedeapsa prevăzută de legea română este detențiunea pe viață ori închisoarea mai mare de 10 ani*. În celelalte cazuri, legea penală română se aplică infracțiunilor săvârşite în afara teritoriului țării de către un cetățean român sau de o persoană juridică română, *dacă fapta este prevăzută ca infracțiune şi de legea penală a țării unde a fost săvârşită ori dacă a fost comisă într-un loc care nu este supus jurisdicției niciunui stat*." Şi art. 10 C. pen. „Legea penală română se aplică infracțiunilor săvârşite în afara teritoriului țării de către un cetățean străin sau o persoană fără cetățenie, contra statului român, *contra unui cetățean român ori a unei persoane juridice române*".

[220] Aşa cum se vede în jurisprudența internațională: cazul acuzării în Germania a directorului CompuServe pentru postarea materialelor obscene pe serverul plasat în SUA(Nash N. *Holding CompuServe Responsible,* New York Times, 1996) sau cauza de defăimare pe internet din 2002 Gutnick

Dacă spațiul cibernetic ar fi un spațiu în care oamenii tind să se comporte virtuos, moral, atunci legile aplicabile trebuie să comporte o latură normativă exhaustivă, care să cuprindă toate aspectele posibile ale manifestării de voință în această dimensiune. Un sistem juridic în care legea este respectată numai din teama sancțiunii nu este un sistem eficient de organizare a comportamentului uman. În esență, dreptul cibernetic nu se poate baza exclusiv pe latura penală a criminalității informatice, ci ar trebui să organizeze şi restul palierelor ce depăşesc sfera incriminatorie, şi de fapt se referă la organizarea socială, la un comportament acceptabil în societate.

Dacă legea națională s-ar aplica doar actorilor spațiului cibernetic aflați într-o anumită locație fizică, nu ne-am confrunta cu problemele procedurale de jurisdicție a raporturilor juridice care se nasc şi se sting exclusiv în spațiul online (de exemplu efectuarea unei vânzări sau cumpărări de pe un site din altă țară, bunul fiind localizat într-o a treia țară). Una din viziunile predominante asupra normelor aplicabile acestui spațiu, este că nu sunt şanse reale de a reglementa la nivel național un domeniu care nu este caracterizat prin naționalitate[221]. Totuşi, asupra chestiunilor care se petrec pe teritoriul național, statele au legitimitatea de a organiza activitățile on-line care determină efecte juridice în limitele granițelor lor[222].

Problema care se pune asupra teritorialității jurisdicției este din perspectiva noilor tehnologii[223], întrucât spațiul fizic în care se află persoana vizată de măsuri de culegere de informații nu coincide cu locația în care se realizează culegerea de informații, sau cu beneficiarul acelor informații. Prin aceasta se poate observa că logica juridică de a califica o faptă a unei persoane după locul în care se săvârşeşte nu mai poate da rezultate eficiente odată transpus în spațiul digital. Jurisdicția unui stat nu mai poate fi un element definitoriu în calificarea corectă a situației de fapt, atâta timp cât internetul nu se supune vreunei jurisdicții.

Emblematice pentru această situație sunt cauza *Weber şi Saravia* contra *Germaniei*[224] şi *Liberty şi alții* contra *Regatului Unit*[225]. În primul caz, reclamanții

---

contra Dow Jones la Curtea Supremă din Australia, sau cauza *Playboy Enterprises* contra *Frena* privind încălcarea dreptului de autor şi concurență neloială pe internet judecat de Curtea districtuală mijlocie din Florida în 1992.

221 Johnson D.R., Post D.G. *Law and Borders – The Rise of Law in Cyberspace,* Stanford Law Review, vol. 48, 1996, p. 1367.

222 Mody S.S. *National Cyberspace Regulation: Unbundling the concept of jurisdiction,* Stanford Journal of International Law, vol. 37, 2001, p. 371.

223 Nast C., *Interference-Based Jurisdiction Over Violations of the Right to Privacy*, EJIL: Talk!, 21.11.2013.

224 Dna Weber, cetățean german care trăieşte în Montevideo, Uruguai, este jurnalist independent care se preocupă de supravegherea realizată de Serviciul de Informații Federal, şi călătoreşte des în Europa. Dl Saravia, cetățean uruguaian lucrează la consiliul local din Montevideo. Acesta a corespondat prin mesaje telefonice cu la dna Weber indiferent unde se afla dumneaei. Cauza a fost decisă în 2006, cu respingerea pretențiilor formulate de reclamanți, iar ingerința în viața privată a celor doi a fost considerată necesară într-o societate democratică.

225 Organizațiile nonguvernamentale irlandeze şi cea britanică s-au plâns că între 1990 şi 1997 corespondența poştală şi comunicațiile electronice le-au fost interceptate de Ministerul de Apărare

trăiau în Uruguai când comunicațiile le-au fost interceptate în Germania, situație în care Curtea de la Strasbourg nu a găsit fundamentată cererea, iar în al doilea caz dintre reclamanți erau organizații irlandeze pentru drepturi civile care corespondau cu una britanică, iar comunicațiile le-au fost interceptate prin autorizația Secretarului de stat privind afacerile interne din Regatul Unit, fiind acuzat că a încălcat prevederile art. 8 din Declarația universală a Drepturilor Omului găsind că sunt insuficiente garanții împotriva unui abuz de putere.

În competiția privind reglementarea rolului guvernelor în domeniul datelor digitale, se remarcă avansul luat de regimurile autoritare[226]. În timp ce statele democratice asociază internetul cu drepturile şi libertățile cetățeneşti, regimurile autoritare au profitat de schimbările şi inovațiile din lumea digitală pentru a-şi consolida controlul, exploatând şi manipulând informațiile vehiculate. Modele noi de guvernanță digitală urmăresc extinderea suveranității asupra spațiului cibernetic, mai exact exercitarea controlului guvernamental asupra datelor şi a internetului în aceeaşi măsură în care se manifestă asupra teritoriului național. Atribuirea unei apartenențe teritoriale datelor a făcut obiectul unor legi care urmăreau extinderea suveranității asupra domeniului cibernetic, exprimată prin cerința ca datele sau domeniile să opereze fizic sau să fie accesibile instituțiilor dintr-o anumită țară. Aceste politici afectează fluxul trans-național de date şi comerțul internațional. Ele oferă regimurilor autoritare acces unic la date de identificare a persoanelor sau la datele comerciale, mărind capacitatea de control a statului[227].

Cea mai afectată componentă a spațiului cibernetic de *reglementarea fracturată la nivel național* este reprezentată de comerțul electronic, care se bazează pe industria comunicațiilor, aşadar pentru Legiuitor provocarea este de a reglementa spațiul cibernetic într-o manieră care să nu constrângă dezvoltarea în plan local. Deci, fluxul de date care tranzitează multiple zone geografice, este susceptibil de a fi condiționat de existența echipamentelor fizice (noduri de comunicații)[228].

Ca antiteză a principiului extrateritorialității din cazul aparte ce ține de politică externă şi diplomație, fluxurile de date vehiculate on-line sunt susceptibile de a face obiectul legii locale. Această interpretare, prin care se acordă *teritorialitate datelor* este o componentă principală a *strategiilor de control a informațiilor* exercitată în state nedemocratice.

Britanic, iar autorizația pusă în executare nu oferea destule garanții pentru o justă apărare în fața justiției britanice. Curtea a decis în 2008 că le-a fost încălcat dreptul la confidențialitatea corespondenței şi la o viață privată.

[226] Marele firewall chinezesc a constituit o sursă de inspirație pentru rețeaua Halal iraniană, dar şi pentru Rusia, fiind adusă în discuție instituirea unui internet separat de cel global. Fenomenul de fracturare a internetului a căpătat denumirea de „splinternet".

[227] Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019, p. 50.

[228] Reed C. *Internet Law: Text and Materials,* ed. 2, Cambridge University Press, 2004, pp. 173-261.

Obligativitatea stocării datelor la nivel național[229] şi accesul nerestricționat al instituțiilor statului la acestea permit guvernelor autoritare să mențină controlul asupra populației şi a informațiilor în limitele frontierelor statale. În mod diferit, Uniunea Europeană impune realizarea cadrului legal pentru garantarea protecției datelor şi vieții private cu accent pe responsabilitatea companiilor comerciale asupra categoriilor de informații gestionate. GDPR promovează, pentru prima oară, norme specifice pentru securitate şi viața privată a persoanelor într-un mod integrat, oferind un precedent pentru reglementarea democratică a protecției datelor private ca drept fundamental. Identificarea şi analiza dreptului aplicabil datelor vehiculate în spațiul digital, respectiv stabilirea autorităților competente să gestioneze amenințările din spațiul cibernetic, sunt direct legate de modalitatea de instituire a unui regim juridic al acestor tipuri de date în plan național, dar şi de angajamentele luate în plan internațional[230].

În acelaşi sens, de a avea un cadru unitar, Comisia Europeană a lansat noua Strategie europeană privind datele electronice prin care se stabileşte ca obiectiv pentru 2025 realizarea unui spațiu european unic al datelor, o piață comună în care să circule liber *datele ne-private* pentru a veni în sprijinul companiilor, cercetării şi administrației publice, care să fie accesibile nelimitat. Totodată, documentul pune în plan central protecția intereselor cetățenilor față de metodele de culegere a informațiilor private accentuând rolul respectării drepturilor fundamentale ale omului. În acest scop Uniunea Europeană propune construirea unui cadru legal puternic pe latura protecției dreptului la viață privată, a protecției drepturilor omului, a siguranței şi a securității cibernetice şi pe altă latură piața internă a datelor gestionate de companiile private. Mai mult, vor trebui îmbunătățite structurile de guvernanță pentru gestionarea datelor şi creşterea disponibilității informațiilor. „Pentru a lansa adevăratul potențial al Europei este necesară realizarea echilibrului între fluxuri de date şi varietatea de utilizare a acestora, în timp ce menținem confidențialitatea, securitatea, siguranța şi **standardele de etică la un nivel ridicat**"[231].

---

[229] Controlul datelor vehiculate la nivel național a fost introdus prin reglementări specifice securității cibernetice: Legile din domeniul mass-media din **Vietnam** şi **Thailanda**, implică elemente de cenzură, în mod special în privința retoricii anti-guvernamentale. **Kazahstanul** a impus, în 2005, ca toate domeniile .kz să opereze pe servere aflate pe teritoriul țării. În **Iran**, componentele controlului informațional exercitat asupra populației sunt reprezentate de cenzura digitală extinsă şi solicitarea de păstrare la nivel local a datelor aplicațiilor WhatsApp şi Telegram. Aceste metode de „naționalizare" a datelor au fost preluate şi de **Turcia** unde Legea de protecție a datelor limitează transferul datelor personale în exteriorul țării, obligând ca unele categorii de date să fie reținute local. **China** şi-a extins abordarea, de la blocarea categoriilor de informații care intră şi ies din țară, la controlul tipului de discuții purtate pe teritoriul său. În 2019 **Rusia** a anunțat planul de a se deconecta de la sistemul global de internet şi de a crea un spațiu virtual rusesc - Runet. (Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019, p. 53).

[230] Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019, p. 54.

[231] Comisia Europeană, *A European strategy for data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 66, 19.02.2020, pp. 2-5.

Modelul Chinei este reprezentat de o extindere a abordării controlului asupra spațiului cibernetic începută cu *marele firewall*[232], la blocarea categoriilor de informații care intră şi ies din țară şi la controlul tipului de discuții purtate în interiorul granițelor geografice ale țării. Legea privind securitatea cibernetică a Republicii Populare Chineze[233], care a intrat în vigoare în luna iunie 2017, extinde teritorialitatea datelor la „infrastructura informațiilor critice" (comunicații publice, energie, finanțe, transport, servicii publice, e-guvernanță etc.) şi implică solicitări de acces la datele gestionate de companii străine, dar şi stocarea şi reținerea datelor sensibile în limitele teritoriale chineze.

Timp de peste 10 ani China a depus un efort susținut ca să obțină date importante rezultate în urma activității derulate de corporațiile străine la nivel local. Această lege restrânge şi mai mult activitatea companiilor prin impunerea unor condiții rigide şi interzicerea accesului pe piața națională. Apple[234] stochează datele utilizatorilor chinezi şi cheile criptografice de deblocare a conturilor pe serverele din provincia Guizhou. Aceste politici sunt menite să susțină interesele naționale ale Chinei de a dezvolta tehnologia autohtonă şi implicit de a controla guvernamental proprietatea intelectuală de origine externă.

De asemenea, China urmăreşte controlul informației prin accesul deplin la datele de identificare personale, iar pentru atingerea obiectivelor strategice una din metodele implementate este de *astroturfing*[235]: armata chineză ajută la promovarea retoricii proguvernamentale lansând în media şi forumurile online mesaje menite să izoleze comentariile negative.

La nivel internațional, China caută să se prezinte ca o apărătoare a deschiderii, siguranței şi cooperării, în acest sens este şi *Strategia internațională pentru spațiul cibernetic* din 2017. În momentul lansării strategiei China anunța, prin intermediul

---

[232] **Marele firewall** a fost pus în practică din 2013 şi este operat de Administrația Spațiului Cibernetic Chinez controlată de Partidul Comunist Chinez, şi care are rolul de propaga viziunea acestuia dar şi de a elimina viziunile contrare. Marele firewall al Chinei este un sistem de supra-veghere prin care se blochează tehnologic accesul populației la site-uri externe. Guvernul explică existența acestui sistem prin exercitarea „suveranității asupra internetului" – „pe teritoriul chinez, internetul este sub jurisdicția suveranității chineze" (O'Brien D. *China's Global Reach: Surveillance and Censorship Beyond the Great Firewall,* Electronic Frontier Foundation, 2019).

[233] Această lege reprezintă o evoluție față de strategia implementată de legea precedentă întrucât de această dată se adresează şi companiilor străine, adică extinde suveranitatea teritorială a internetului chinez, către actorii privați ce intră în legătura cu spațiul cibernetic chinez. (Xia L, Leo Z., *China's Cybersecurity Law: An Introduction for Foreign Businesspeople,* China Briefing, 2018)

[234] Nellis S, Cadell C, *Apple moves to store iCloud keys in China, raising human rights fears*, Reuters, 2018.

[235] Este o tehnică folosită pe social media prin care se propagă mesaje de dezinformare fără a arăta finanțatorul respectivei campanii, păstrând aparența originalității utilizatorilor. În esență, este o **tehnică de dezinformare**. (Lyon T.P., Maxwell J.W. *Astroturf Lobbying,* Journal of Economics & Management Strategy, 2004).

site-ului guvernului[236], că îşi propune să ajute statele în curs de dezvoltare să îşi dezvolte capacitățile de securitate cibernetică şi să contribuie la reglementarea domeniului cibernetic global. Unul din cele patru principii pe care se bazează strategia este „suveranitatea" (pe lângă pace, guvernanță comună, şi beneficii comune).

De asemenea, controlul chinez asupra populației este exercitat, într-o mare măsură, prin ***sistemul de credite sociale***, în care, totalitatea datelor personale şi comerciale sunt supravegheate constant pentru a realiza *profilul unei persoane sau al unei companii*[237]. În funcție de acesta pot fi aplicate sancțiuni persoanelor sau companiilor neperformante precum interzicerea accesului la servicii bancare, la anumite locuri de muncă, la facilități de transport sau alte servicii sociale[238].

Această colecție guvernamentală de metadate a folosit confidențialitatea utilizatorilor dincolo de ceea ce realizează alte state prin intermediul politicilor publice eficiente şi al procesului democratic[239].

Modelul Rusiei este reprezentat de colectarea, controlul şi supravegherea datelor digitale în mod constant, din acest motiv au fost dezvoltate variate regimuri juridice pentru a pune în practică politica de stat, chiar dacă ele afectează sectorul privat.

Doctrina de securitate a informației[240] din 2016 schițează abordarea holistică a Kremlinului, care include integrarea tehnologiei şi a componentelor psihologice pentru controlul informației digitale. De cele mai multe ori tacticile ce privesc securitatea informației sunt testate în plan național înainte de a fi folosite în plan extern[241].

Pentru a obține suveranitatea cibernetică, Rusia a folosit *Legea datelor private* din 2015[242] care impunea ca orice date ale cetățenilor săi să fie stocate pe servere

---

[236] http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm accesat pe 20.02.2020.

[237] Botsman R. *Big Data se întâlneşte cu Big Brother pe măsură ce China se ocupa cu evaluarea cetățenilor*, Wired UK, 2017.

[238] Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019,

[239] Lascateu C. *The collision between public policy and technology raises the stakes for users*, IKS 2018 Security and Freedom - Contemporary European Policies and Future Perspectives, RISR, no. 19-20/2018, 2019, pp. 411-416.

[240] Care înlocuieşte doctrina anterioară adoptată în 2000. Cele 3 principii de bază sunt reprezentate de contracararea amenințărilor externe, învingerea discriminării media ruseşti de factori internaționali şi depăşirea limitărilor tehnologice pe care le înfruntă Rusia în domeniul tehnologiei informației.
https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 accesat la 15.01.2020.

[241] Lascateu C., *Obiectivele Războiului hibrid rus,* Geopolitica, anul XVI, nr. 74 2/2018.

[242] Prima formă de reglementare a datelor private în Rusia a fost realizată în 2006 şi chiar de atunci impunea operatorilor de servicii de comunicații să implementeze măsuri organizatorice şi tehnice pentru protecția acestui tip de date.

din țară. O nouă lege, din 2016, a extins controlul impunând păstrarea timp de 6 luni a comunicațiilor utilizatorilor[243]. Operatorii de servicii de internet şi telecomunicații au fost obligați să refuze furnizarea de servicii către utilizatorii care nu vor să își dezvăluie identitatea, la solicitarea instituțiilor de aplicare a legii[244].

Rusia a cerut totodată companiilor străine să predea codurile sursă pentru produsele de securitate drept contraprestație pentru afacerile desfăşurate în acest spațiu. Recent, Rusia a anunțat intenția clară de a se deconecta de la sistemul global de internet şi de a crea un spațiu virtual rusesc – Runet[245].

Două reglementări din 2017 întăresc controlul asupra datelor, eliminând posibilitatea anonimității online şi legitimează instrumentele de restricționare a rețelelor virtuale private sau de anonimizare care au ca scop eludarea cenzurii[246]. Totodată, companiei Facebook i s-a cerut să detalieze cum se conformează acestor legi, crescând presiunea asupra altor corporații străine pentru a le determina să accepte noile reglementări.

Media condusă de stat joacă un rol-cheie în *Strategia de securitate a informației*, promovând dorința de a obține suveranitatea cibernetică şi teritorialitatea datelor. Pretinzând implementarea granițelor virtuale, statul rus îşi asumă rolul de moderator şi protector al datelor private împotriva accesului ilegal. La începutul anului 2018, Roskomnadzor (autoritatea rusă de reglementare în comunicații) a blocat milioane de adrese IP în tentativa de a opri funcționarea platformei Telegram, după refuzul acesteia de a furniza autorităților cheile de criptare a mesajelor. În contextul scandalului mediatic ce a urmat, televiziunea de stat anunța sfârşitul globalizării şi al anonimității odată cu inevitabila instituire a granițelor virtuale. Plasarea sub o singură autoritate a supravegherii stocării datelor la nivel național, a cenzurii şi dezinformării demonstrează multitudinea măsurilor active ale Rusiei pentru controlul informației[247].

CONSIDERAȚII FINALE

Ceea ce se remarcă este faptul că fiecare stat are propria viziune asupra securității naționale, drept urmare, programele de supraveghere realizate de o rețea de servicii secrete care transmit informații transfrontalier, în timp ce caută să

---

[243] *Processing and Storage of Personal Data in the Russian Federation. Changes since September 1, 2015*, Ministerul Telecomunicațiilor din Rusia, 12.02.2016 https://digital.gov.ru/en/personaldata/ accesat la 13.01.2020.

[244] *Freedom of the Net 2016: Russia Country Profile,* Freedom House, 2016.

[245] Alternativa rusească la internetul global. (Wakefield J. *Russia „Successfully tests" its unplugged internet,* BBC, 24.12.2019).

[246] *Internet Anonymity Will Soon Disappear, Russian Culture Minister Warns*, The Moscow Times, 21.01.2019.

[247] Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019.

îşi satisfacă propriile interese naţionale arată o aplecare spre latura politică a relaţionărilor interstatale, şi mai puţin pe latura de drept internaţional în forma tratatelor şi acordurilor de alianţă.

Imaginea clasică a modelului bazat pe contractul social survenit într-o anarhie a relaţiilor inter-statale pare a fi cea mai apropiată de ceea ce reprezintă spaţiul digital pentru actori statali şi omenire, ţinând cont, pe de-o parte, că, în esenţă, etica în contextul culegerii de informaţii descrie maniera în care comunităţi specifice, unite de factorul comun reprezentat de domeniul profesional, fundamentează şi operaţionalizează în norme specifice culturale, cutume şi practici, valorile lor morale, iar, pe de altă parte, folosirea tehnologiei şi a părţii fizice a internetului (cabluri şi hub-uri) ca sursă de informaţii a cărei poziţionări geografice naşte avantajul politic al statului respectiv, generează totodată şi schimbări în influenţa exercitată internaţional în termeni de putere statală.

În răspuns faţă de aceste politici s-au dezvoltat strategiile altor actori de a rezista acestor politici prin instrumente precum diplomaţia şi aplicarea dreptului internaţional, dar şi prin influenţarea comportamentului uzual al utilizatorilor de internet (Rusia, China, Turcia).

Chiar şi aşa, tratatele internaţionale nu sunt interpretate la nivel statal într-o modalitate care să reflecte dorinţa de limitare a culegerii de informaţii din comunicaţii, iar în practică, dorinţa de a include *viaţa privată digitală* în reglementările internaţionale confirmă faptul că normele existente nu sunt interpretate ca norme ce privesc supravegherea electronică ca fapt, ci implicaţiile politice care apar din această activitate realizată de instituţii statale.

Faptul relevant pentru această analiză este că normele actuale pivotează în jurul *informaţiilor care duc la identificarea persoanei*, spre exemplu Organizaţia de Cooperare Economică şi Dezvoltare (OECD) subliniază în procedurile sale că „date personale reprezintă orice date care duc la o persoană identificată sau identificabilă" pe când protecţia datelor în Uniunea Europeană adaugă faptul că „o persoană identificabilă direct sau indirect, mai ales în legătură cu un număr de identificare sau mai mulţi factori specifici identităţii sale: fizic, psihologic, mental, economic, cultural sau social".

Chiar dacă această abordare se dovedeşte a fi eficientă pentru procesarea tradiţională a datelor cu caracter privat, în *era big data* acestea necesită a fi suplimentate şi cu privire la *identificarea bazată pe caracteristici ale categoriilor de persoane şi a grupurilor*[248].

Ideea vine în contextul în care politicile publice şi deciziile se fundamentează pe profiluri şi tipare ale unor grupuri, şi nu pentru un individ anume, aşadar ar trebui luat în calcul dacă grupul respectiv prosperă, dacă poate acţiona autonom, dacă este tratat du respect etc.

---

[248] Taylor L., Floridi L., van der Sloot B. *Group Privacy: new challenges of data technologies*, Springer, 2017, p. 14.

Ca rezultat, o viziune ar fi ca primele forme de normativ internațional care ar trebui să apară ar trebui să aibă un puternic caracter procedural, mai puțin general, care să se aplice domeniului de culegere de informații, şi mai puțin asupra tipului de date private la care se referă şi felului în care are impact asupra vieții private. Beneficiul acestei abordări constă în faptul că ar putea fi mai bine verificate sub aspectul legalității respectivele măsuri. Totodată, această abordare continuă linia de gândire trasată în secolele precedente, bazată pe necesitatea delimitării clare a excepțiilor de la aplicarea normei generale – *exceptio est strictimissimae interpretationis*[249].

Indiferent care ar fi modalitatea de a stabili cadrul legal al supravegherii informatice a vieții private în plan internațional, aceasta ar trebui să urmărească următoarele linii directoare: în primul rând, normele ar trebui să *sporească transparența regulilor aplicabile*, generând astfel şi o jurisprudență unitară.

În al doilea rând, acest cadru normativ ar trebui să *minimizeze arbitrariul*, acest aspect fiind strâns legat de *transparentizarea procedurilor şi a modalității de stabilire a țintelor supravegherii*.

În al treilea rând, aceste reguli ar trebui să *crească responsabilitatea instituțiilor implicate* precum şi a celor responsabili de politicile de stat privind securitatea națională.

Mai mult, ar trebui redusă, dacă nu eliminată, *distincția dintre cetățeni şi străini* în protecția persoanelor şi a garanțiilor oferite asupra dreptului la viață privată.

Deopotrivă, un element care se dovedeşte a fi critic privind comunitatea de informații din state democratice este reprezentat de mijloacele de control extern, independent[250]. Prin definiție, publicul nu poate fi un factor direct de responsabilizare a serviciilor pentru că aproape întreaga activitate a acestora se petrece în secret.

Aşa cum reține Hegel[251] în lumina gândirii aristoteliene bazate pe experiența anterioară „oricare ar fi înțelepciunea sau adevărul pe care putem să îl studiem din istorie, acestea sunt atât de întinse cât este şi prezentul în istorie şi timp", dacă ne uităm spre trecut pentru a estima potențialul spațiului cibernetic ca resursă pentru societate există şanse să rămânem antamați într-un cadru depăşit, când abordarea acestui domeniu ar trebui să fie realizată din perspectiva tehnologiilor emergente.

---

[249] Din latină „excepția este de strictă interpretare", însemnând că nu se pot aduce excepții de la aplicarea legii prin interpretare sau analogie, cazurile în care nu este aplicabilă norma generală trebuie exact stipulate în actul normativ sau în contract, aspect subliniat şi de jurisprudența CJUE în cauza Weil şi Gulacsi împotriva Ungariei, Cehiei, Poloniei, 2019.

[250] Cauza *Klass împotriva Germaniei* în care s-au supus analizei prevederile legale naționale privind supravegherea țintite asupra persoanelor CEDO a reținut că se impune instituirea unui mijloc de control independent (1978).

[251] Georg Wilhelm Friedrich Hegel – filosof idealist german din secolul XIX care arată că între necesitate şi libertate este doar o aparentă opoziție.

BIBLIOGRAFIE

Publicații on-line
1. https://www.abc.net.au
2. http://snowdenandthefuture.info
3. https://dcssproject.net
4. https://supreme.justia.com/cases
5. https://nakedsecurity.sophos.com
6. https://www.privacyrules.com
7. https://eur-lex.europa.eu
8. https://www.echr.coe.int
9. https://www.consilium.europa.eu
10. http://www.europarl.europa.eu
11. https://en.wikipedia.org
12. http://www.statewatch.org
13. https://www.jstor.org
14. https://www.ecchr.eu
15. https://www.osce.org

Curtea Europeana a Drepturilor Omului *(cronologic)*:
16. *Klass împotriva Germaniei,* 1978,
17. *Gaygustus* împotriva *Austriei,* 1996,
18. *Bancovic şi alții* împotriva *Belgiei şi alții,* 2001,
19. *Coster* contra *Regatului Unit al Marii Britanii,* 2001,
20. *Von Hannover* contra *Germaniei*, 2004,
21. *Weber şi Saravia* contra *Germaniei,* 2006,
22. *Pfeifer* contra *Austriei*, 2007,
23. *Liberty şi alții* contra *Regatului Unit,* 2008,
24. *A şi alții* împotriva *Secretarului de Stat pentru Afaceri Interne,* 2009,
25. *Big Brother Watch* contra *Regatului Unit al Marii Britanii,* 2018,
26. *Catt* împotriva *Regatului Unit*, 2019,

Curtea de Justiție a Uniunii Europene
27. *Digital Rights Ireland* contra *Irlandei şi alții,* 2014,
28. *Schrems* contra *Comisarul de protecție a datelor Irlanda*, 2015,
29. *Secretarul de Stat pentru Afaceri Interne* împotriva *Watson,* 2016,
30. *Tele2 Sverige AB* împotriva *Post,* 2016,
31. *Privacy International* şi alții, 2017,
32. *Ordre des barreaux francophones et germanophone* şi alții, 2018,
33. *La Quadrature du Net şi alții,* 2018,
34. *Weil şi Gulacsi* împotriva *Ungariei, Cehiei, Poloniei*, 2019,

Curtea Internațională de Justiție

35. *Timorul de Est* împotriva *Australiei*, 2015-42, 2013-16

Curtea Supremă a Regatului Unit

36. *A şi alții* împotriva *Secretarului de Stat pentru Afaceri Interne*, 2004 (cazul Belmarsh)

37. *Catt* împotriva *Regatului Unit*, 2015

38. *Secretarul de Stat pentru Afaceri Interne* împotriva *Watson,* 2016

Curtea Supremă a Statelor Unite ale Americii (*cronologic*)

39. *Olmstead* împotriva *SUA,* 1928

40. *Katz* împotriva *SUA,* 1967

41. *Statele Unite* împotriva *Verdugo-Urquidez,* 1990

Curtea Supremă a Australiei

42. *Gutnick* contra *Dow Jones*, 2002,

Curtea Constituțională a României

43. Decizia nr. 1258/2009 referitoare la admiterea excepției de neconstituționalitate a prevederilor Legii nr. 298/2008 *privind reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum şi pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice*

44. Decizia nr. 440/2014 referitoare la excepția de neconstituționalitate a dispozițiilor Legii nr. 82/2012 *privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice şi de furnizorii de servicii de comunicații electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice şi ale art. 152 din Codul de procedură penală*

Reglementări (*cronologic*):

45. Acordului multilateral de cooperare în domeniul SIGINT dintre Australia, Canada, Noua Zeelandă, Regatul Unit şi Statele Unite ale Americii, din 1941, înnoit în 1943,

46. Declarația universală a drepturilor omului, 1948 - Adunarea generală a Consiliului Organizației Națiunilor Unite,

47. Convenția pentru apărarea Drepturilor Omului şi a Libertăților Fundamentale (Convenția Europeană a Drepturilor Omului) 1950 (intrată în vigoare în 1953) -Adunarea generală a Consiliului Organizației Națiunilor Unite,

48. Pactul internațional cu privire la drepturile civile şi politice ale omului 1966 (intrată în vigoare în 1967) – Consiliul Europei,

49. Legea privind viața privată 1974, SUA

50. Comentariul 16: articolul 17 (dreptul la viață privată) dreptul la respectarea vieții private, a familiei, a căminului şi a corespondenței şi protecția onoarei şi a reputației adoptată în cea de-a 32-a sesiune a Comitetului pentru drepturile omului, Organizația Națiunilor Unite, 08.04.1988.

51. Decizia Comisiei Europene 2000/520/EC prin care se constată conformitatea principiilor de transfer a datelor cu caracter personal între SUA şi UE cu Directiva 95/46/EC,

52. Constituția României, 1990, revizuită în 2003,

53. Legea nr. 51/1991 *privind securitatea națională*, republicată,

54. Legea nr. 182/2002 privind protecția informațiilor clasificate,

55. Standardele naționale de protecție a informațiilor clasificate în România, aprobate prin Hotărârea de Guvern nr. 585/2002,

56. Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice

57. Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice - Directiva asupra confidențialității şi comunicațiilor electronice

58. Directiva 2006/24 a Parlamentului European şi Consiliului Europei privind *retenția datelor cu caracter personal generate sau procesate în legătură cu serviciile publice de comunicații electronice sau rețele de comunicații publice*, de completare a Directivei 2002/58/EC privind viața privată şi comunicațiile electronice

59. Legea nr.298/2008 privind *reținerea datelor generate sau prelucrate de furnizorii de servicii de comunicații electronice destinate publicului sau de rețele publice de comunicații, precum şi pentru modificarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice*

60. Codul penal 2009,

61. Directiva 2009/1369/EC de modificare şi completare a Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice

62. Legea nr. 82/2012 privind *reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice şi de furnizorii de servicii de comunicații electronice destinate publicului, precum şi pentru modificarea şi completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecția vieții private în sectorul comunicațiilor electronice*

63. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 2013 – Comisia Europeană

64. Codul civil, 2013

65. Codul de procedură penală, 2014

66. Rezoluția Adunării Generale a Organizației Națiunilor Unite referitoare la *Dreptul la viață privată în Era Digitală*, nr. 68/167, 21.01.2014,

67. Rezoluția Parlamentului European *EU Strategic Communication to Counteract Anti-EU Propaganda by Third Parties*, 2016/2030,

68. Regulamentul (UE) 2016/679 publicat în Jurnalul Oficial al Uniunii din 04.05.2016 – Parlamentul European – GDPR,

69. Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor şi privind libera circulație a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului,

70. Ordinul Executiv al preşedintelui Trump „Creşterea siguranței publice în interiorul SUA" nr.13768 din 25.01.2017,

71. OSCE, *OSCE shares experiences with Organization of American States on how to enhance interstate co-operation, transparency, predictability and stability in cyberspace*, 2018,

72. European Data Protection Supervisor, *Online manipulation and personal data*, *Opinion*. 3, 2018,

73. Camera Reprezentanților din Senatul Statelor Unite ale Americii, *Raportul comunității de informații privind măsurile active ruseşti,* 22.03.2018,

74. Opinia Consiliului Uniunii Europene privind îmbunătățirea reținerii datelor în scopul luptei împotriva criminalității nr. 7833/19 din 27.03.2019,

75. Opinia Consiliului Uniunii Europene asupra aplicării GDPR pentru Comisia Europeană nr.12991/19 din 15.10.2019,

76. Comisia Europeană, *A European strategy for data*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 66, 19.02.2020,

Publicații (*alfabetic*):

77. Ainuvee K., *The Impact of Snowden's Revelations on the Perception of the US*, Tallinn, 2013,

78. Asser M. *Echelon: Big Brother without a cause?* BBC, 06.06.2000,

79. Arredy J.T. *China Aims to Rewrite Rules of Global Web,* Wall Street Journal, 2015,

80. Baer D.B., *The European Union as a Partner Against Russian Aggression: Sanctions, Security, Democratic Institutions and the Way Forward,* Declarația depusă în fața Senatului SUA, Comitetul pentru Relații Externe, 04.04.2017,

81. Bauman Z., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. *After Snowden: Rethinking the Impact of Surveillance,* International Political Sociology, nr.8, 2014,

82. Bamford J. *The NSA Is Building the Country's Biggest Spy Center. Watch What You Say*, Wired, 15.03.2012,

83. Bigo D., *Raportul privind securitatea națională şi probele secrete în legislație şi în fața instanțelor: explorarea dificultăților* Comisia Parlamentului European pentru libertăți civile, justiție şi afaceri interne (LIBE), 2014,

84. Bittman L., *The KGB and Soviet Disinformation: An Insider's View*, Washington: Pergamon-Brassey's, 1985,

85. Botsman R. *Big Data se întâlneşte cu Big Brother pe măsură ce China se ocupa cu evaluarea cetățenilor*, Wired UK, 2017,

86. Brandeis L., Warren S., *The Right to Privacy*, The Harvard Law Review nr.4/5, 1980,

87. Brimmer S.E., *The Role of Ethics in 21st Century Organizations* Leadership Advance online, nr. XI, 2007,

88. Burns J.H., *Happiness and Utility: Jeremy Bentham's Equation*, Utilitas. 2005,

89. Charluet C., *It's possible to monetize data while respecting consumer privacy – here's how*, Growth, 2019,

90. Chen A., *The Agency*, The New York Times, 02.06.2015,

91. Chivvis C.S., *Understanding Russian "Hybrid Warfare" and What Can Be Done About it*, RAND Corporation, CT-468, Testimony presented before the House Armed Services Committee 22.03.2017,

92. Cioclei V., *Manual de criminologie* C.H. Beck, 2019,

93. Clarke R.A., *Liberty And Security in a Changing World*, US Review Group on Intelligence and Communications Technologies, 12.12.2013,

94. Cohn C., Kayyali N. *The Top 5 Claims That Defenders of the NSA Have to Stop Making to Remain Credible.* Electronic Frontier Foundation, 2014,

95. Coleman S., *Even dirtier Hands in War: Considering Walser's Supreme Emergency Argument,* Research in Ethical Issues in Organisations, 2015,

96. Comisia de la Veneția *The Report on the Democratic oversight of the Security Services* adoptat la cea de-a 71-a sesiune Plenară, Veneția, 1-2.06.2007,

97. Constantinescu M., Iorgovan A., Murau M., Tănăsescu E.S., *Constituția României revizuită comentarii şi explicații,* All Beck, 2004,

98. Deleuze G., *Postscript on the Societies of Control,* The MIT Press, vol.59, 1992,

99. Departamentul de Stat al SUA, *A Report on Active Measures and Propaganda*, 1986 - 1987, Washington: Department of State Publication, 1987,

100. Dicționarul explicativ al limbii române, ed. 2, Academia Română, Institutul de Lingvistică, Univers Enciclopedic Gold, 2009,

101. Dicey A.V., *Introduction to the study of the law of the constitution,* Library of Congress Cataloging in Publication Data, ed. 8, Macmillan, Londra, 1915,

102. Dipert R.R., *The Essential Features for an Ontology for Cyberwarfare, Conflict and Cooperation in Cyberspace,* CRC Press, 2013,

103. Dorell O., *Alleged Russian Political Meddling Documented in 27 Countries Since 2004*, USA Today, 2017

104. *Factbox: Who is Cambridge Analytica and what did it do?,* Reuters, 23.03.2018,

105. Fischer B., *Okhrana: The Paris Operations of the Russian Imperial Police*, Diane Publishing, 1999,

106. Franklin B., Saprks J., Franklin W.T. *The life of Benjamin Franklin: containing the Autobiography, with notes and a continuation,* Whittemore, Niles and Hall, 31.12.1856,

107. *Freedom of the Net 2016: Russia Country Profile,* Freedom House, 2016,

108. Fried C., *Privacy*, Yale Law Journal, ed.3, vol. 77, 1968,

109. Fuller L.L., *The morality of Law,* ed.2, Yale University Press 1969,

110. Gallagher R., *Extensive British Spying throughout Africa revealed in Le Monde*, The Intercept, 2016,

111. Galeotti M., *Putin's Hydra: Inside Russia's Intelligence Services*, European Council on Foreign Relations (ECFR), 2016,

112. Galeotti M., *Controlling Chaos: How Russia Manages its Political War in Europe*, European Council on Foreign Relations (ECFR), 2017,

113. Gowder P., *The Rule of Law and Equality,* Law and Philosophy, vol.32, nr. 5, Springer, 2013,

114. Gellman B., *US surveillance architecture includes collection of revealing internet, phone metadata.* The Washington Post, 16.06.2013,

115. Gellman B, DeLong M. *How the NSAs MUSCULAR program collects too much data from Yahoo and Google,* The Washington Post, 28.12.2013,

116. Gellman B., Soltani A. *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, Washington Post, 2013,

117. Granick J. *The Surveillance State's Legalism Isn't about Morals, It's about Manipulating the Rules,* Just Security, 13.11.2013,

118. Gross H., *Privacy and Autonomy* în Pennock şi Chapman (ed.) Nomos XIII, Atherton Press, 1971,

119. Hafetz J. *A Problem of Standards?: Another Perspective on Secret Law,* Willian & Mary Law Review, vol.57, 2016,

120. Harloe K., Neville M. *Thucydides and the Modern World: Reception, Reinterpretation and Influence from Renaissance to the Present*, Cambridge University Press, 2012,

121. Harris S, Hudson J., Lynch C. *Germany, Brazil Turn to UN to Restrain American Spies*, Foreign Policy, 25.10.2013,

122. Hersh S.M. *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, New York TIMES, 22.12.1974,

123. Ionescu D. *Geolocation 101: How It Works, the Apps and Your Privacy*, PCWorld, 29.03.2010,

124. *Internet Anonymity Will Soon Disappear, Russian Culture Minister Warns*, The Moscow Times, 21.01.2019,

125. *Is More Gridlock Just a Hack Away?* Washington Post, 09.08.2015,

126. Johnson D.R., Post D.G. *Law and Borders – The Rise of Law in Cyberspace,* Stanford Law Review, vol. 48, 1996,

127. Kant I., *The Metaphysics of Ethics*, 1785,

128. Keane B. *Open and shut: ASIS crime and the Labor Liberal cover-up,* Crikey, 12.06.2015,

129. Koskenniemi M., *From Apology to Utopia: The Structure of International Legal Argument,* Cambridge University Press, 2006,

130. Kovalev A., Bodner M., *The Secrets of Russia's Propaganda War, Revealed*, The Moscow Times, 2017,

131. Khrennikov I., *Russia Threatens to Shut Facebook Over Local Data Storage Laws*, Bloomberg Technology, 26.09.2017,

132. Kutz C., *Secret Law and the Value of Publicity,* Ratio Juris vol.22, nr.2, 2009,

133. Latimer J. *A commodity-Form Critique of Mass Surveillance,* Tallinn, 2017,

134. Lascateu C., Medeşan A. *YouTube şi combaterea radicalizării*, Revista Intelligence nr. 35, 2017,

135. Lascateu C., *Social media takes a toll on Democracy,* Redefining Community in Intercultural Context, Henri Coandă Air Force Academy Publishing House, 2018,

136. Lascateu C., *Obiectivele Războiului hibrid rus,* Geopolitica, anul XVI, nr. 74 2/2018,

137. Lascateu C. *The collision between public policy and technology raises the stakes for users*, IKS 2018 Security and Freedom - Contemporary European Policies and Future Perspectives, RISR, no. 19-20/2018, 2019,

138. Lascateu C. *Date şi state. Controlul teritoriului digital*, Revista Intelligence nr. 39, 2019,

139. Lauterpacht H. Sir, *The Function of Law in the International Community,* Oxford, 1933,

140. Lloyd S.A., Sreedhar S. *Hobbes s Moral and Political Phiosophy,* Stanford Encyclopedia of Philosophy, 12.02.2012,

141. Lowenthal C., *Intelligence: From Secrets to Policy*, ed. 7, CQ Press, 2017,

142. Lynch C., Harris S., Hudson J. *Germany, Brazil Turn to U.N. to Restrain American Spies,* Foreign Policy, 14.10.2013,

143. Lubin A. *Espionage as a Sovereign Right under International Law and its Limits*, ILSA, vol 24, nr. 3, 2016,

144. Lucas G., *Ethics and Cyber Warfare. The Quest for Reasonable Security in the Age of Digital Warfare,* Oxford University Press, 2017,

145. MacIntyre A. *Intractable Disputes about the Natural Law: Alasdair MacIntyre and critics,* University of Notre Dame, 2009

146. McChesney R., Foster J.B. *Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age*. vol. 66 nr. 3 Monthly Review iulie -august 2015,

147. Medine D., *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*. Privacy and Civil Liberties Oversight Board 2014,

148. Michael M.G., Michael K., *National Security: The Social Implications of the Politics of Transparency,* University of Wollongong, 2006,

149. Milanovic M., *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, Harvard International Law Journal, vol.56, nr.1, 2015,

150. Mody S.S. *National Cyberspace Regulation: Unbundling the concept of jurisdiction,* Stanford Journal of International Law, vol. 37, 2001

151. Moglen E., *Snowden and the Future*: *Part IV*; Freedom's Future, 2013,

152. Moore J.N. *Solving the War Puzzle: Beyond the Democratic Peace,* Carolina Academic Press, 2017,

153. Montefiore S., *The Romanovs*, Knopf A.A., 2016,

154. Nash N. *Holding Compuserve Responsible*, New York Times, 1996

155. Nast C., *Interference-Based Jurisdiction Over Violations of the Right to Privacy*, EJIL: Talk!, 21.11.2013,

156. Nellis S, Cadell C, *Apple moves to store iCloud keys in China, raising human rights fears*, Reuters, 2018,

157. Northcott C., *The Role, Organisation and Methods of MI5*, International Journal of Intelligence and Counterintelligence nr.20/3, 2007,

158. Oboler A., Welsh K., Cruz L. *The danger of big data: Social media as computational social science,* First Monday, 2012,

159. O'Brian D. *China's Global Reach: Surveillance and Censorship Beyond the Great Firewall,* Electronic Frontier Foundation, 2019

160. Omand D. Sir, *Mass Electronic Surveillance and Liberal Democracy,* Research Centre in International Relations, Department of War studies, King s College London, 21.01.2014,

161. Parent W.A., *Privacy, Morality and the Law*, Philosophy and Public Affairs vol.12/4, 1983,

162. Pennock J.R., Chapman J.W., *Privacy: Nomos* ed. XIII Atherton Press, 1971,

163. Pentland. A. *Society s nervous system: building effective government, energy and public health systems,* Pervasive and Mobile Computing, vol. 7, nr. 6, 2011,

164. Piel S., Tilouine J. *British spying: tentacles reach across Africa's heads of states and business leaders*, Le Monde, 2016,

165. *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, A Minority Staff Report Prepared for The Use of The Committee on Foreign Relations United States Senate, U.S. Government Publishing Office, 10.01.2018.

166. Raine A., Yang Y. *Neural foundations of moral reasoning and antisocial behavior*. Social Cognitive and Affective Neuroscience, nr. 1, vol.3, 2006,

167. Reed C. *Internet Law: Text and Materials,* ed. 2, Cambridge University Press, 2004,

168. Rödl şi partenerii, *Legea privind confidențialitatea datelor din India şi GDPR al Uniunii Europene*, 24.05.2018,

169. *Russia Censors Media by Blocking Websites and Popular Blog*, The Guardian, 14.03.2014,

170. *Russia Passes Law to Force Websites onto Russian Servers*, Reuters, 04.07.2014,

171. Sánchez-Bordona C. *The means and methods of combating terrorism must be compatible with the requirements of the rule of law*, comunicat de presă nr. 4/20, CJUE,15.01.2020,

172. Sanger D.E., O'Neil J. *White House Begins New Effort to Defend Surveillance Program*, The New York Times, 23.01.2006,

173. Satter R. şi alții, *Russia Hackers Pursued Putin Foes, Not Just US Democrats*, Associated Press, 02.11.2017,

174. Schlanger M. *Intelligence Legalism and the National Security Agency s Civil Liberties Gap,* University of Michigan Law School Scholarship Repository, 2015,

175. Schoen F., Lamb J. C., *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference***,** Strategic Perspectives, 2012,

176. Sferle A. *Limbajul juridic şi limba comună,* Universitatea Tibiscus Timişoara, Universite Paris III Sorbonne Nouvelle, 2005,

177. Shils E., *Privacy: Its Constitution and Vicissitudes*, Law and Contemporary Problems 31/2, ed Universității Duke, 1966,

178. Shklar J. *Legalism: Law, Morals, and Political Trials 1,* Harvard University Press 1964, reed.1986,

179. Soldatov A., Borogan I., *The Red Web: The Kremlin's War on the Internet*, PublicAffairs, 2015,

180. Sprigman C. *The NSA's Culture of "Legal Compliance" Still Breaks the Law*, Just Security, 2014,

181. Stone G. R. Secrecy and Self-Governance, 56 New York Law School Law Review 81, 2011,

182. *Tallinn Manual on the International Law Applicable To Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013,

183. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, ed. 2, Cambridge University Press, 2017.

184. Taylor L., Floridi L., van der Sloot B. *Group Privacy: new challenges of data technologies,* Springer, 2017,

185. Thompson K. *Foucault – Surveillance and Control,* Crime and Deviance, Revise Sociology, 2016,

186. Wakefield J. *Russia „Successfully tests" its unplugged internet,* BBC, 24.12.2019,

187. Watts R. William *Hague: British public have 'nothing to fear' from US spies*, The Telegraph, 09.06.2013,

188. Weinstein M.A. *The Uses of Privacy in the Good Life,* Privacy: Nomos XIII, Atherton, 1971,

189. Westin A.F., *Privacy and Freedom*, ed. Bodley Head, Londra, 1967,

190. Whitehead T., *New powers to record every phone call and email makes surveillance '60m times worse*, Telegraph, 2012,

191. Wilkinson M, Cronau P. *Drawing the Line,* ABC, 24.03.2014,

192. Xia L, Leo Z., *China's Cybersecurity Law: An Introduction for Foreign Businesspeople,* China Briefing, 2018,

193. Yannakogeorgos P., *The Prospects for Cyber Deterrence: American Sponsorship of Global Norms, Conflict and Cooperation in Cyberspace: The Challenge to National Security,* US Air Force Research Institute, 2013,

194. Zeng M. *Metadata Types and functions* NISO 07.10.2016,

195. Zuboff S. *Big other: surveillance capitalism and the prospects of an information civilization*, Journal of Information Technology, 2015.