CRJM | CENTRUL DE RESURSE JURIDICE DIN MOLDOVA

str. Şciusev 33, MD-2001 Chişinău, Republica Moldova; tel: +(373) 22 843 601; fax: +(373) 22 843 602; web: www.crjm.org

Opinie cu privire la proiectul de lege nr. 161 pentru modificarea și completarea unor acte legislative (legea „Big Brother")[1]

Data: 23 noiembrie 2016

Conținut

[1] Opinia a fost elaborată de Bogdan Manolea, în colaborare cu Centrul de Resurse Juridice din Moldova (CRJM), în cadrul proiectului „Promovarea mecanismelor eficiente de responsabilizare a judecătorilor în Moldova", implementat de CRJM cu suportul financiar al Programului de Drept al Fundației Soros-Moldova. Opiniile exprimate în acest document aparțin în exclusivitate autorului şi nu reflectă neapărat poziția instituției finanțatoare.

Centrul de Resurse Juridice din Moldova (CRJM) este o organizație non-profit neguvernamentală, cu sediul în Chișinău, Republica Moldova. CRJM promovează asigurarea unei justiții calitative, prompte și transparente. În realizarea acestui obiectiv, CRJM combină cercetarea de politici și activitatea de advocacy realizate într-un mod independent și neutru. CRJM a fost implicat în elaborarea mai multor documente de politici publice și acte normative.

Bogdan Manolea este jurist specializat pe domeniul dreptului tehnologiei informației de peste 15 ani, cu interes pentru modul cum tehnologia interferează cu drepturile omului, dar și de orice domeniu implicând dreptul, Internetul și atitudinea civică. Bogdan este proprietarul paginii web Legile Internetului - legi-internet.ro, care prezintă din 2001 principalele evoluții din dreptul tehnologiei informației, și Directorul Executiv al Asociației pentru Tehnologie și Internet - ApTI. Bogdan este autor a peste 150 de prezentări și articole pe teme legate de Drept și Tehnologia Informației, prezentate la evenimente naționale și internaționale.

Sumar:

Legea nr. 161 pentru modificarea și completarea unor acte legislative (denumită legea „Big Brother") ridică mai multe probleme generale și punctuale în ceea ce privește modul cum aceste reglementări ar putea fi aplicate, dar și care ar putea aduce atingere drepturilor fundamentale, și a dreptului la viața privată în special, fără a fi justificate ca fiind necesare într-o societate democratică conforme practicii Curții Europene a Drepturilor Omului (CtEDO).

Astfel în vreme ce în Uniunea Europeană (UE) se discută despre limitarea măsurilor de supraveghere generalizată (*mass surveillance*) în contextul deciziilor Curții Europene de Justiție (CJUE)[2] și a 4 curți constituționale din UE[3] privind legi de păstrare a datelor de trafic informațional, este de rău augur faptul că în Republica Moldova se propun noi legi de extindere a obligațiilor de păstrare a traficului informațional fără o analiză completă cu privire la necesitatea ingerinței în drepturile fundamentele.

Mai mult, includerea unor modificări din mai multe domenii și zone de interes în mai multe acte normative – unele poate întemeiate, altele cu siguranță discutabile și cu efecte asupra drepturilor fundamentale – ridică semne de întrebare legitime cu privire la necesitatea fiecărei măsuri în parte și măsura în care este fundamentată această necesitate.

Pentru a lua un singur exemplu în acest sumar, aplicarea concretă a propunerii de sistare a accesului la „toate adresele IP pe care sunt amplasate pagini web (…) ce conțin informații care îndeamnă la ură sau discriminare națională, rasială ori religioasă, la ostilitate sau violență" ar duce în mod direct la blocarea Facebook, YouTube sau Twitter în Republica Moldova, deși suntem siguri că nu aceasta a fost dorința legiuitorului.

Recomandările noastre punctuale pe fiecare articol sunt detaliate mai jos, însă în general ar fi legate de:

- renunțarea la articolele propuse ce ar însemna măsuri de supraveghere generalizată (cum ar fi cele legate de păstrarea traficului informațional, în special Art. VI p. 2 al proiectului nr. 161 (modificarea art. 247[1] Codul Contravențional); Art. VII p. 6 (modificări la art. 7 al Legii nr. 20 privind prevenirea şi combaterea criminalității informatice, în special problematice în alineatul (1) litera a), c), f), h));
- analiza punctuală a legislației care extinde limitarea drepturilor fundamentale, inclusiv cu un studiu de impact asupra drepturilor omului bazat pe jurisprudența și expertiza CtEDO;
- renunțarea la obligațiile de „sistare" a accesului la paginile web. Această activitate de blocare prin ISP a paginilor web reprezintă o interferență în traficul normal de internet între utilizatori și pagini web ce ridică probleme de încălcare a libertății de exprimare și a dreptului la viață privată, prin crearea unui strat de cenzură. Este important să înțelegem diferența tehnică între:

---

[2] Hotărârea CJUE în cauza C-362/14 Maximillian Schrems/Data Protection Commissioner http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf și Hotărârea CJUE din 8 aprilie 2014 în cauzele conexate C-293-12 şi C-594-12 *Digital Rights Ireland* *http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=RO*.

[3] Decizia 1258/2009 a Curții Constituționale din România- http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html; Decizia Curții Constituționale din Slovacia (2014): http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-us-102014-78; Decizia Curții Constituționale din Cehia (2011): http://www.usoud.cz/en/decisions/20110322-pl-us-2410-data-retention-in-telecommunications-services/; Decizia Curții Constituționale din Germania (2010): http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.

- Sistarea accesului/blocarea – caz în care conținutul rămâne pe Internet, este vizibil pentru majoritatea utilizatorilor, dar este ascuns celor din Republica Moldova care sunt supuși blocării.
- Ștergerea conținutului de pe Internet – caz în care conținutul ilegal nu mai poate fi găsit online.

Considerăm că soluția corectă poate fi doar ștergerea materialelor ilegale, corelată cu o investigație penală pentru identificarea infractorilor care au făcut imaginile și/sau le-au publicat online ;

- clarificarea terminologică, păstrarea neutralității tehnologice în exprimare și explicitarea clară a termenilor folosiți în funcție de tehnologie;
- încurajarea colaborării voluntare pentru raportarea de infracțiuni informatice.

Analiza proiectului de lege și recomandări punctuale:

Proiectul de lege pentru modificarea și completarea unor acte legislative, adoptat de Guvern la 11 aprilie 2016, înregistrat la Parlament, la 13 aprilie 2016, cu nr. 161 (*în continuare „proiectul nr. 161”*) ridică mai multe probleme generale și punctuale în ceea ce privește modul cum aceste reglementări ar putea fi aplicate, dar și care ar putea aduce atingere drepturilor fundamentale, și a dreptului la viața privată în special, fără a fi justificate ca fiind necesare într-o societate democratică conforme practicii Curții Europene a Drepturilor Omului (CtEDO).

În acest sens prezentăm șapte chestiuni generale de importanță deosebită ce trebuie luate în considerare la un astfel de act normativ, urmat de o serie de probleme punctuale majore pe textul prezentat public.

A. Chestiuni generale

Necesitatea oricărei ingerințe în drepturile fundamentale trebuie să fie demonstrată

În primul rând considerăm că orice act normativ care aduce în mod inerent limitări ale drepturilor fundamentale trebuie însoțită de o analiză exhaustivă de impact asupra acestora. Astfel **orice ingerință în exercițiul unui drept**, deci și al dreptului la viață privată, pentru a fi considerată de către CtEDO conformă cu **Convenția europeană pentru drepturile Omului (CEDO), trebuie să îndeplinească, cumulativ, următoarele criterii:**

- ingerința trebuie să fie prevăzută de lege;
- ingerința trebuie să urmărească un scop legitim;
- ingerința trebuie să fie necesară într-o societate democratică;
- ingerința trebuie să fie proporțională cu scopul urmărit.

Astfel, nota informativă a proiectului de lege trebuie să demonstreze în mod cumulativ cum sunt justificate aceste elemente pentru orice articol sau element din reglementare care aduce atingere vieții private. Nota proiectului 161 este lacunară și nu are nicio analiză a impactului asupra drepturilor omului.

Orice text care prevede o ingerința trebuie să fie clar și precis

Subliniem obligația că orice ingerință în dreptul la viață privată trebuie să fie legală, adică trebuie să fie "*prevăzută de lege*", care include și faptul că legea trebuie să fie de o anumită calitate. În acest sens, CtEDO a dezvoltat două cerințe principale: legea care limitează dreptul la viață privată trebuie să fie suficient de clară, precisă și previzibilă, și în plus să fie accesibilă.

Claritatea, precizia și previzibilitatea legii înseamnă că legea trebuie să fie "*formulată cu destulă precizie pentru a permite unui cetățean să decidă conduita sa și să prevadă, în mod rezonabil, în funcție de circumstanțele*

cauzei, consecințele care ar putea rezulta dintr-un fapt determinat"[4].

În contextul special de interceptare a comunicațiilor în scopul anchetelor poliției, CtEDO notează că "*legea trebuie să fie suficient de clară în ceea ce privește posibilitatea de a da cetățenilor, în general, o indicație corespunzătoare cu privire la împrejurările și condițiile în care autoritățile publice sunt împuternicite să recurgă la această intervenție secretă și potențial periculoasă asupra respectării vieții private și a corespondenței* "[5].

Mai mult, CtEDO consideră că "*dreptul material în sine, spre deosebire de însoțirea practică administrativă,* ***trebuie să indice domeniul de aplicare și modalitățile de exercitare ale acestei puteri discreționare cu suficientă claritate, având în vedere scopul legitim al măsurii în cauză****, pentru a oferi individului o protecție adecvată împotriva arbitrarului*"[6].

În acest context notăm că textul propus folosește de multe ori termeni neclari, dincolo de actele normative internaționale citate ca motivație (*spre exemplu,* „prestator servicii poștă electronică sau mesagerie textuală", „sistarea accesului", includerea în aceeași categorie a datelor cu privire la traficul informațional și datelor de conținut, obligația de ținere a evidenței utilizatorilor de servicii, etc.), ceea ce nu îndeplinește cerințele clarității textelor actelor normative. Mai multe comentarii în acest sens sunt incluse în observațiile punctuale, mai jos.

Textele documentelor internaționale trebuie coroborate cu alte acte normative internaționale colaterale

Textul propus pare a prelua literalmente dispoziții din Convențiile internaționale și a le interpreta într-o singură direcție, fără a ține cont de corelarea acestora cu alte acte normative colaterale. De exemplu, Convenția privind criminalitatea informatică de la Budapesta precizează în Preambul importanța corelării Convenției cu restul reglementărilor și recomandărilor ce privesc protecția vieții private și a datelor cu caracter personal:

„- conștiente de necesitatea garantării unui echilibru adecvat între interesele acțiunii represive și respectarea drepturilor fundamentale ale omului, consacrate prin Convenția ***Consiliului Europei pentru apărarea drepturilor omului și a libertăților fundamentale (1950)****, Pactul internațional privind drepturile civile și politice al Națiunilor Unite (1966), precum și prin alte tratate internaționale aplicabile în materia drepturilor omului, care reafirmă dreptul fiecăruia la opinie, libertatea de expresie, precum și libertatea de a căuta, de a obține și de a comunica informații și idei de orice natură, fără a ține seama de frontiere, precum și drepturile privind respectarea intimității și a vieții private,*

- conștiente, de asemenea, de dreptul la protecția datelor personale, conferit, de exemplu, prin Convenția ***Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (1981)****,*
(...)
- reamintind recomandările Comitetului Miniștrilor (...) nr. ***R (87) 15 vizând reglementarea utilizării datelor cu caracter personal în sectorul poliției, nr. R(95)4 privind protecția datelor cu caracter personal în domeniul serviciilor de telecomunicații, cu referire specială la serviciile de telefonie*** *(...)"*

Astfel toate aceste dispoziții trebuie să fie corelate în modul de aplicare a dispozițiilor Convenției de la Budapesta, aspect ce lipsește în totalitate din textul propus. De asemenea această Convenție internațională nu

---

[4] CtEDO, Sunday Times *vs. Marea Britanie,* 26 April 1979, § 49.

[5] CtEDO, *Malone vs. Marea Britanie*, 2 august 1984, citată în Council of Europe, *Case Law of the European Court of Human Rights Concerning the Protection of Personal Data*, 30 Jan. 2013 (DP (2013) CASE LAW), p. 19.

[6] CtEDO, *Malone vs. Marea Britanie*, citat mai sus.

poate reglementa aspecte de detaliu cu privire la modul de implementare, care sunt lăsate la nivelul fiecărui stat membru.

În acest sens, dacă se doresc implementări ale unor articole din Convenția de la Budapesta, trebuie să se implementeze în mod corelativ și dispoziții care reglementează garanțiile prevăzute de Convenție, sau – dacă ele deja există – referințe cu privire la modul cum aceste dispoziții sunt deja prevăzute de legislația din Republica Moldova.

Mai concret, măsurile prevăzute în proiectul 161 trebuie să fie corelate cu:

- respectarea dreptului la viață privată din Convenția Consiliului Europei pentru apărarea drepturilor omului și a libertăților fundamentale (1950) (vezi și pct. I - Necesitatea oricărei ingerințe în drepturile fundamentale trebuie să fie demonstrată);
- legislația din domeniul protecției datelor cu caracter personale, inclusiv normele cu privirea la protecția datelor personale în sectorul polițienesc.

Măsurile de supraveghere generalizată ale tuturor cetățenilor încalcă drepturile fundamentale

În contextul actual al societății informaționale și ca urmare a dezvăluirilor și reacțiilor din ultimii 5 ani, trebuie să facem distincția între supravegherea punctuală (care poate să includă interceptări de comunicații sau acces la meta-date) și supravegherea generalizată care "nu începe cu suspiciunea împotriva unei sau unor persoane anume"[7].

"O reglementare care le permite autorităților publice accesul în mod generalizat la conținutul comunicărilor electronice aduce atingere substanței dreptului fundamental la respectarea vieții private."[8] Aceasta este concluzia Curții Europene de Justiție cu privire la supravegherea generalizată – opinie regăsită în multiple decizii, studii și luări de poziție publice, apărute în special după dezvăluirile lui Snowden.[9]

Proiectul nr. 161 menține, extinde sau introduce obligații de monitorizare generală a tuturor utilizatorilor de comunicații electronice, ceea ce este incompatibil cu drepturile fundamentale, așa cum au concluzionat mai multe curți constituționale, spre exemplu cea din Germania[10], România[11], Cehia[12] sau Slovacia[13], dar și CJUE într-o decizie din 2014, statuând că:

---

[7] A se vedea pentru detalii Raportul Comisiei de la Viena din Martie 2015, intitulat "Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies" disponibil la http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e.

[8] Hotărârea CJUE în cauza C-362/14 Maximillian Schrems/Data Protection Commissioner http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf.

[9] Pentru o listă mai largă a se vedea capitolul "Mass surveillance for the purpose of national security in international law" punctele 3- 16 din Opinia Judecătorului PINTO DE ALBUQUERQUE în CtEDO, *Szabo si Vissy* . Ungariei, 12 ianuarie 2016 (http://hudoc.echr.coe.int/eng?i=001-160020).

[10] Decizia Curții Constituționale din Germania (2010): http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.

[11] Vezi decizia 1258/2009 a Curții Constituționale din România- http://www.legi-internet.ro/jurisprudenta-it-romania/decizii-it/decizia-curtii-constitutionale-referitoare-la-legea-pentru-pastrarea-datelor-de-trafic-298-2008.html

[12] Decizia Curții Constituționale din Cehia (2011): http://www.usoud.cz/en/decisions/20110322-pl-us-2410-data-retention-in-telecommunications-services/.

[13] Decizia Curții Constituționale din Slovacia (2014): http://fra.europa.eu/en/caselaw-reference/slovakia-constitutional-court-slovak-republic-pl-us-102014-78.

"Trebuie să se constate că ingerința în drepturile fundamentale (...) este de o mare amploare și trebuie considerată ca fiind deosebit de gravă. În plus, împrejurarea că păstrarea datelor și utilizarea lor ulterioară sunt efectuate fără ca abonatul sau utilizatorul înregistrat să fie informați cu privire la aceasta este susceptibilă să genereze în mintea persoanelor vizate (...), sentimentul că viața lor privată face obiectul unei supravegheri constante".[14]

În Uniunea Europeană au fost deja anulate acte normative majore care au propus măsuri de supraveghere generalizată, cum sunt Directiva privind păstrarea datelor de trafic informațional, dar și acordul Safe Harbour de transfer de date între SUA și UE.

Mai mult, măsurile de supraveghere generalizată nu și-au dovedit niciodată eficacitatea. Spre exemplu, Adunarea Parlamentară a Consiliului Europei a notat că în conformitate cu "evaluările independente realizate în Statele Unite, supravegherea generală se pare că niciodată nu a contribuit la prevenirea atacurilor teroriste, contrar afirmațiilor anterioare făcute de funcționari de rang înalt din domeniul securității. În schimb, resursele care ar fi putut preveni atacuri sunt direcționate pentru supraveghere generală, lăsând persoanele potențial periculoase să acționeze liber"[15].

Blocarea adreselor IP de către ISP reprezintă o măsură de cenzură a Internetului

Cerința de blocare (în textul original se folosește termenul incorect de sistare[16], spre ex. art. VI al proiectului de lege nr. 161, care modifică art. 247[1] Codul Contravențional; art. VII al proiectului de lege nr. 161, care modifică art. 7 lit. h) din Legea privind prevenirea și combaterea criminalității informatice a unor adrese IP de către furnizorul de servicii Internet (ISP), ridică numeroase probleme de „privatizare a aplicării legii" și a creării unei infrastructuri de cenzură, în special în contextul neclarității asupra a cine va crea și menține lista respectivă și pe ce criterii, dar și a punerii în aceeași categorie a situațiilor extrem de diferite din punct de vedere tehnic (găzduire vs. intermediare).

Problema fundamentală este că blocarea site-urilor web prin intermediul furnizorului de servicii Internet constituie o măsură de cenzură a conținutului online, măsură ce ridică probleme serioase în ceea ce privește respectarea drepturilor omului în general și a dreptului la liberă exprimare în particular.

În acest sens Uniunea Europeană a inclus în directiva privind comunicațiile electronice obligația pentru statele membre ca accesul la Internet să nu poată fi blocat sau limitat în mod abuziv. Articolul 1 alin. (3a) din Directiva 2002/21/CE prevede în mod explicit că:

> *„**Măsurile luate de statele membre cu privire la accesul utilizatorilor finali** la serviciile și aplicațiile prin rețele de comunicații electronice sau cu privire la utilizarea acestor servicii și aplicații de către utilizatorii finali **trebuie să respecte drepturile și libertățile fundamentale** ale persoanelor fizice, astfel cum sunt garantate de Convenția Europeană pentru apărarea drepturilor omului și a libertăților fundamentale, precum și principiile generale ale dreptului comunitar."*

Internetul și site-urile web sunt unanim recunoscute ca mijloace de comunicare în public, astfel blocarea

---

[14] Hotărârea CJUE din 8 aprilie 2014 în cauzele conexate C-293-12 şi C-594-12 *Digital Rights Ireland.*

[15] Par. 11 din Rezoluția nr. 2045 (2015) a Adunării Parlamentare a Consiliului Europei, din 21 aprilie 2015, disponibilă la http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en.

[16] Sistarea accesului la o adresa IP – în sens de oprire, încetare sau întrerupere se poate face tehnic doar de instituția care administrează adresele IP, în cazul României RIPE NCC – https://www.ripe.net/, care are proceduri specifice de alocare sau relocare de adrese IP - https://www.ripe.net/publications/docs/ripe-643.

acestora în mod arbitrar riscă să contravină CEDO și Constituției Republicii Moldova Art. 34 aliniatul (5), care prevede că *„Mijloacele de informare publică nu sunt supuse cenzurii”.*

Faptul că proiectul 161 are precizate condiții neclare când un anumit site nu trebuie să fie accesat de către utilizatori ridică probleme ale constituționalității acestei dispoziții.

Lipsa de claritate a legii în ceea ce privește soluțiile tehnice pentru blocare (cu diferite implicații pentru viața privată, așa cum am menționat mai sus) face imposibilă studierea proporționalității măsurii de blocare a Internetului. Cu toate acestea CtEDO menționează în jurisprudența sa că inclusiv blocarea doar a anumitor site-uri este problematică și “nu îi diminuează semnificația, în special din momentul când Internetul a devenit unul dintre principalele mijloace prin care indivizii își exercită dreptul la libertatea de exprimare și informare, mijloc ce oferă unelte esențiale pentru participarea în activități și discuții despre aspecte politice sau de interes general.”[17]

De asemenea, Raportorul ONU cu privire la libertatea de exprimare concluzionează[18] cu privire la acest subiect că: **“*Măsurile de blocare constituie o modalitate inutilă și disproporționată de a atinge scopul declarat*”.**

Din punct de vedere tehnic, sunt deja documentate cazuri la nivel mondial în care, în funcție de metoda tehnică folosită, blocarea a dus la imposibilitatea accesului la site-uri 100% legale, dar găzduite pe același IP, sau la blocarea unui site întreg (de ex. Wikipedia[19] sau Tumblr[20]) pentru un singur conținut discutabil.

Mai mult decât atât, implementarea unui astfel sistem de blocare a site-urilor de către furnizorii de servicii Internet înseamnă că sunt create și puse în funcțiune o serie de instrumente de cenzură care pot fi extinse foarte ușor la alte domenii. Odată acceptată blocarea Internetului și odată ce este pus la punct un sistem tehnic pentru implementarea acesteia, din ce în ce mai mulți vor cere ca din ce în ce mai multe lucruri să fie cenzurate.

În acest context, din punctul nostru de vedere, accentul trebuie să se pună pe identificarea cazurilor de pornografie infantilă pe Internet și ștergerea acestui conținut (și nu blocarea lui, care înseamnă doar ascunderea sa[21]), eventual prin aderarea la rețelele internaționale similare de hotline-uri (vezi INHOPE). De asemenea eforturi deosebite trebuie făcute în special pentru prinderea infractorilor care au abuzat de acei copii în viața reală, pentru a preveni repetarea acțiunilor infracționale.

Obligativitatea înregistrării unor servicii electronice este o măsură cel puțin discutabilă

Deși proiectul nr. 161 prevede doar chestiuni adiacente la acest subiect, considerăm important de precizat că obligativitatea înregistrării utilizatorilor unor servicii conform art. 7 din legea privind prevenirea și combaterea criminalității informatice nr. 20-XVI din 03.02.2009 și prevederea de sancțiuni pentru ne-implementarea acestei obligații presupune că accesarea oricărui serviciu electronic este posibil doar după ce utilizatorul respectiv s-a

---

17 CtEDO, *Ahmet Yıldırım c. Turciei*, 6 aprilie 2004 și *Cengiz și Ceilalți c. Turciei*, 1 decembrie 2015.

18 Frank LaRue, “Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression”, A.HRC.17.27, http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

19 A se vedea, spre exemplu, cazul din Marea Britanie din 2008, descris aici - http://www.theregister.co.uk/2008/12/07/brit_isps_censor_wikipedia/.

20 A se vedea, spre exemplu, cazul din Italia din 2013 - http://history.edri.org/edrigram/number11.4/italy-blocks-tumblr-domain.

21 Pentru mai multe argumente a se vedea detalii la MOGIS - Scoate, nu bloca! -- Acționează şi nu întoarce capul! - https://mogis.info/archive/eu/ro/**.**

înregistrat într-un fel sau altul (aspect care nu este detaliat).

O astfel de abordare este, pe de o parte, contrară principiilor generale ale colectării datelor cu caracter personal[22], obligând înregistrarea utilizatorilor chiar și dacă furnizorul acelui serviciu nu dorește acest lucru. Pe de altă parte, o asemenea obligație este iluzorie, câtă vreme furnizarea serviciilor pe Internet nu este supusă vreunei înregistrări, deci cetățenii moldoveni pot oricând să apeleze la un furnizor din afara Republicii Moldova, eludând prevederile acestea. Mai mult, există servicii pe Internet unde anonimitatea este un aspect cheie al furnizării acelor servicii – de la servicii de tip VPN sau un serviciu de a raporta fapte de corupție ori chiar raportarea de conținut de tip pornografie infantilă pe Internet.

Internetul este un spațiu descentralizat – legea ar putea fi inaplicabilă

Proiectul de lege nr. 161 nu ține cont de structura de rețea descentralizată și nelimitată la nivel statal a Internetului**.** Astfel reglementările mult prea stricte în condițiile în care Republica Moldova este un actor relativ mic în zona Internetului, nu va duce decât la o legislație inaplicabilă (pentru că furnizorii străini vor refuza aplicarea unor prevederi care fac disonanță față de legislația lor națională) și la trimiterea utilizatorilor din Republica Moldova către alte servicii în afara celor naționale.

Mai mult, aceste măsuri (de genul „ținerii în evidență a utilizatorilor de servicii" sau „accesarea materialelor de pornografie adultă cu bună știință în locuri publice") pot funcționa în detrimentul firmelor de servicii online și cetățenilor moldoveni, prin ușurința arbitrarului unor astfel de încălcări ale legii.

Este nevoie de o lege care să modifice așa de multe aspecte?

Din punct de vedere formal, subliniem că modalitatea de a adopta un act normativ ce modifică alte 7 acte normative[23] cu privire la aparenta implementare a mai multor convenții internaționale – unele obligatorii, altele facultative – din domenii diferite (protecția copiilor, combaterea criminalității informatice, etc.) ridică semne de întrebare cu privire la eficacitatea acestei măsuri, în special cu privire la motivarea și dezbaterea proiectului, dar și a argumentației cu privire la necesitatea cumulării lor într-un singur act normativ.

B. Opinii punctuale cu privire la cele mai importante propuneri la proiectul de lege nr. 161

1. Art. II p. 4 (art. 259 alin. (1) Codul penal), p. 7 (art. 260[2]), p. 8 (art. 260[3] alin. (1)), p. 9 (art. 260[4] alin. (1)), p. 11 (art. 260[6] alin. (1)), p. 12 (art. 261[1] alin. (1)) din proiectul nr. 161, care prevăd excluderea următoarelor cuvinte din dispozițiile alineatelor enumerate: cuvintele „(și) dacă aceste acțiuni au cauzat daune în proporții mari."

Considerăm că limitarea unor infracțiuni informatice doar la cele care produc "daune în proporții mari", așa cum sunt reglementate în prezent, era de bun augur, în condițiile în care textul infracțiunii este extrem de larg și

[22] A se vedea în acest sens Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, deschisă spre semnare pentru statele membre ale Consiliului Europei la Strasbourg la 28 ianuarie 1981, ratificată de Republica Moldova și intrată în vigoare de la 1 iunie 2008 (în special Art. 5), dar și Legea nr. 133 privind protecția datelor cu caracter personal din 8 iulie 2011 (în special art 4).

[23] Proiectul nr. 161 modifică următoarele acte normative: (1) Codul penal; (2) Codul de procedură penală; (3) Legea nr. 264 din 27.10.2005 cu privire la exercitarea profesiunii de medic; (4) Legea nr. 241 din 15.11.2007 a comunicațiilor electronice; (5) Codul contravențional; (6) Legea nr. 20 din 03.02.2009 privind prevenirea și combaterea criminalității informatice; (7) Legea nr. 59 din 29.03.2012 privind activitatea specială de investigații.

există posibilitatea de a primi foarte multe plângeri care să inunde organele de urmărire penală. De exemplu "modificarea de date informatice" fără drept poate să îmbrace o gamă foarte largă de acțiuni întâlnite în practică, astfel procurorii vor trebui să discearnă în fiecare caz dacă fapta are un pericol social suficient de mare pentru a fi considerată infracțiune. Eventual se poate discuta în ce infracțiuni o astfel de măsură ar avea sens din punct de vedere practic, după o analiză detaliată a tipologiilor de infracțiuni care ar scăpa procesului penal. De asemenea, se poate stabilit o limită mai mică dacă se consideră că există o anumită topologie caracteristică infracțiunilor din Republica Moldova.

<u>În concluzie, recomandăm menținerea textului actual al dispozițiilor art. 259 alin. (1), art. 260^2, art. 260^3 alin. (1), art. 260^4 alin. (1), art. 260^6 alin. (1) și art. 261^1 alin. (1), care includ ca element al componenței de infracțiune „dacă aceste acțiuni au cauzat daune în proporții mari". Respectiv, art. II p. 4, 7, 8, 9 și 11 ale proiectului nr. 161 urmează a fi excluse sau revizuite.</u>

<u>2. Art. III p. 1, care prevede completarea Codului de procedură penală cu articolul 130^1 cu următorul cuprins: „Articolul 130^1 . Percheziția informatică și ridicarea obiectelor care conțin date informatice".</u>

Sugerăm efectuarea unei analize detaliate a modului cum acest articol urmează a fi aplicat, în vederea asigurării unui text care ar respecta cu strictețe dreptul la viața privată.

De asemenea, recomandăm completarea art. 130^1 cu următoarele:

- La alin (5), care privește măsura de extindere a percheziției pentru un "alt sistem informatic ori suport de stocare a datelor informatice", recomandăm să se facă în aceleași condiții procedurale ca și percheziția inițială, eventual incluzându-se un element de celeritate**. Având în vedere afectarea drepturilor fundamentale ale persoanei în momentul unei percheziții informatice, este importantă păstrarea nivelului de autorizare de la judecător**, chiar dacă acest aspect ar putea duce uneori la prelungirea investigației penale. Având în vedere faptul că în practică nu se lucrează pe un sistem informatic deschis, în principal pentru că aceasta duce la alterarea inerentă a informațiilor prelucrate, estimăm că astfel de cazuri vor fi destul de puțin prezente în practică, mai ales dacă se dorește respectarea condiției de a fi "realizat prin intermediul unor metode şi mijloace tehnice ce asigură integritatea şi autenticitatea informațiilor conținute în acestea."
- recomandăm **includerea obligației exprese de a se efectua copii pentru toate obiectele ridicate, la momentul ridicării și în prezența martorilor și a persoanei căreia îi aparțin datele** și a se face analiza doar pe acestea, în vederea asigurării integrității datelor informatice, dar și pentru a permite o contra-expertiză reală în orice moment al procesului și dovedirea faptului că datele originale nu au fost alterate în cadrul procesului de ridicare, stocare sau percheziție (*chain of custody*). Obligația respectivă ar putea fi inclusă la alin. (3) din art. 130^1;
- având în vedere că pe obiectele ridicate vor exista în majoritatea cazurilor și alte informații cu referire la viața personală a unor persoane implicate în cauză, ca și la informații ce nu privesc ancheta pentru care se face percheziția, **considerăm că trebuie să existe o obligație expresă pentru organele de urmărire penală de confidențialitate și restituire a acestor date imediat ce este constatat faptul că acestea nu sunt pertinente cauzei examinat**e, astfel ca aceste informații să nu devină publice în mod nejustificat. Obligația de confidențialitate și restituire imediată a datelor urmează a fi prevăzută expres în art. 130^1 Codul de procedură penală.

<u>3. Art. III p. 2, care prevede extinderea aplicării unei serii de măsuri speciale de investigație la toate infracțiunile grave, deosebit de grave și excepționale de grave și la o serie de infracțiuni mai puțin grave.</u> Și anume, se propune aplicarea următoarelor măsuri speciale de investigație, prevăzute de Codul de procedură penală (CPP):

- Cercetarea domiciliului şi/sau instalarea în el a aparatelor ce asigură supravegherea şi înregistrarea audio şi video, a celor de fotografiat şi de filmat (art. 132^6 CPP),
- Supravegherea domiciliului prin utilizarea mijloacelor tehnice ce asigură înregistrarea (art. 132^7 CPP),
- Documentarea cu ajutorul metodelor şi mijloacelor tehnice, localizarea sau urmărirea prin sistemul de poziționare globală (GPS) ori prin alte mijloace tehnice (art. 134^3 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*),
- Reţinerea, cercetarea, predarea, percheziţionarea sau ridicarea trimiterilor poştale (art. 133 CPP),
- Identificarea abonatului, proprietarului sau utilizatorului unui sistem de comunicaţii electronice ori al unui punct de acces la un sistem informatic (art. 134^5 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*),
- Colectarea informaţiei de la furnizorii de servicii de comunicaţii electronice (art. 134^4 CPP),
- Urmărirea vizuală (art. 134^6 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*),
- Achiziția de control (art. 138^3 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*),
- Investigația sub acoperire (art. 136 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*),
- Supravegherea transfrontalieră (art. 138^1 CPP, *notă: efectuată doar cu autorizarea procurorului conform art. 132^2 CPP*).

la următoarele infracțiuni:

- există o bănuială rezonabilă cu privire la pregătirea sau săvârșirea unei infracţiuni grave, deosebit de grave sau excepțional de grave, cu excepțiile stabilite de lege SAU în cazul infracțiunilor prevăzute de
- art. 174 - Raportul sexual cu o persoană care nu a împlinit vîrsta de 16 ani,
- art. 175 – Acțiuni perverse,
- art. 175^1 – Ademenirea minorului în scopuri sexuale,
- art. 185^1 – Încălcarea dreptului de autor şi a drepturilor conexe,
- art. 185^2 – Încălcarea dreptului asupra obiectelor de proprietate industrială,
- art. 208^1 – Pornografia infantilă,
- art. 208^2 - Recurgerea la prostituţia practicată de un copil,
- art. 237 – Fabricarea sau punerea în circulaţie a cardurilor sau a altor instrumente de plată false,
- art. 259 - Accesul ilegal la informaţia computerizată,
- art. 260 - Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program,
- 260^1 - Interceptarea ilegală a unei transmisii de date informatice.

La detalierea normelor prevăzute de art. III p. 2 al proiectului de lege nr. 161 este evidentă extinderea infracțiunilor pentru care pot fi aplicate măsurile speciale de investigație, inclusiv cele aplicate doar cu autorizația procurorului.

În opinia noastră, **extinderea** acestor măsuri cu privire la o categorie extrem de largă de infracțiuni grave și mai puțin grave **trebuie să fie justificată punctual, pentru fiecare infracțiune în parte,** pentru ca avem de a face cu o extindere a limitării drepturilor fundamentale, care nu poate fi justificată în mod generic în conformitate cu practica constantă a CtEDO.

În același timp este evident că **anumite infracțiuni din această listă** (cum ar fi cele de "acces ilegal la informație computerizată", "simpla deținere de materiale pornografice cu minori" sau cele legate de încălcarea drepturilor de autor pot fi foarte ușor folosite în alt scop sau relativ ușor de înfăptuit de către orice persoană și, mai ales în

acest context, **nu par a avea gravitatea** prevăzută de lege pentru asemenea măsuri și, respectiv, pot fi folosite în mod abuziv extrem de ușor.

În concluzie, recomandăm limitarea listei de infracţiuni pentru care pot fi aplicate măsurile speciale de investigaţie, respectiv modificarea art. III p. 2 al proiectului de lege nr. 161.

4. Art. III p. 3, care prevede completarea Articolul 138[2] din Codul de procedură penală (livrarea controlată) cu alineatul (7) cu următorul cuprins: „Măsura specială de investigaţii prevăzută de prezentul articol poate fi dispusă în cazul infracţiunilor prevăzute la art. 132[1] alin. (2) pct. 2) din prezentul cod sau al unei infracţiuni prevăzute la art. 175[1], 185[1] -185[2], 208[1], 208[2], 237, 260-260[2], 260[4], 260[6] şi 261[1] din Codul penal."

Considerăm că lista infracțiunilor pentru care se permite aplicarea măsurii speciale de investigații „livrare controlată" este prea largă și urmează a fi revizuită și limitată. Astfel, prin art. III p. 3 al proiectului nr. 161 se propune dispunerea măsurii speciale de investigație livrare controlată în orice caz în care există o bănuială rezonabilă cu privire la pregătirea sau săvârșirea unei infracţiuni grave, deosebit de grave sau excepțional de grave, cu excepțiile stabilite de lege sau în cazul următoarelor infracțiuni prevăzute de Codul penal:

- 175[1] – Ademenirea minorului în scopuri sexuale;
- 185[1] – Încălcarea dreptului de autor şi a drepturilor conexe;
- 185[2] – Încălcarea dreptului asupra obiectelor de proprietate industrială;
- 208[1] – Pornografia infantilă;
- 208[2] - Recurgerea la prostituţia practicată de un copil;
- 237 – Fabricarea sau punerea în circulaţie a cardurilor sau a altor instrumente de plată false;
- 260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program;
- 260[1] - Interceptarea ilegală a unei transmisii de date informatice;
- 260[2] - Alterarea integrităţii datelor informatice ţinute într-un sistem informatic;
- 260[4] - Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similar;
- 260[6] - Frauda informatică şi
- 261[1] - Accesul neautorizat la reţelele şi serviciile de telecomunicaţii.

Autorul proiectului de lege nu a motivat necesitatea prevederii unei măsuri de investigaţie atât de intruzive pentru toate aceste infracţiuni. În special nu este clară includerea acestei măsuri pentru infracțiunile legate de dreptul de autor (art. 185[1] și 185[2]). Recomandăm revizuirea întregii liste, cu justificarea celor menținute și excluderea art. 185[1] și 185[2] din lista infracţiunilor la investigarea cărora poate fi utilizată măsura livrării controlate.

5. Art. III p. 6 din proiectul nr. 161, care prevede introducerea unui noi tip de măsuri speciale de investigaţie – interceptarea şi înregistrarea datelor informatice - modificând art. 132[11] CPP (care în prezent prevede verificarea înregistrării interceptărilor) prin includerea următoarelor norme:

„Articolul 132[11]. Interceptarea şi înregistrarea datelor informatice

(1) Interceptarea şi înregistrarea datelor informatice constă în folosirea unor metode şi/sau mijloace tehnice prin intermediul cărora are loc colectarea în timp real a datelor referitoare la traficul informatic şi/sau a datelor referitoare la conţinut, asociate comunicaţiilor respective, altele decât cele prevăzute în art. 132[8] , transmise prin intermediul unui sistem informatic, şi stocarea informaţiilor obţinute în urma interceptării pe un suport tehnic.

(2) Interceptarea și înregistrarea datelor informatice se dispune și se efectuează în condițiile prevăzute

la art. 132[9], care se aplică în mod corespunzător[24].

(3) Măsura specială de investigații prevăzută de prezentul articol poate fi dispusă în cazul infracțiunilor prevăzute la art. 132[1] alin. (2) pct. 2) din prezentul cod sau al unei infracțiuni prevăzute la art. 175-171[1], 185[1]-185[3], 208[1], 208[2], 237 și 259-261[1] din Codul Penal."

Articolul 132[11] prevăzut la art. III p. 6 al proiectului nr. 161 este neclar în ceea ce privește distincția necesară între date de trafic și date de conținut, și mai ales în ceea ce privește distincția între datele referitoare la conținut din art. 132[11] și datele de comunicare din 132[8] Codul de procedură penală. **În mod logic ar trebui făcută o distincție clară și fără echivoc între** :

- **conținutul comunicărilor**, a cărei interceptare este deja reglementată în art 132[8] ;Din punct de vedere tehnic o comunicare prin sistemul de protocol IP sunt „date de conținut" și
- **datele de trafic**, care par a fi deja reglementate de art. 134[4].

Chiar și Convenția de la Budapesta face distincția între cele două tipuri de date (art. 20 și respectiv 21).

În acest context trebuie să subliniem că **dispozițiile Convenției de la Budapesta nu trebuie implementate literal,** ci doar să existe instituții în dreptul intern care să permită aceste măsuri procedurale, ținând cont de specificul național. În același timp aceste măsuri trebuie să fie circumscrise practicii CtEDO și dispozițiilor constituționale interne, deci din punctul nostru de vedere măsurile legate de datele de trafic (art. 134[4] din Codul de Procedură Penală și art. 7 din Legea privind prevenirea şi combaterea criminalității informatice) ar trebui să fie revăzute în contextul deciziilor constituționale[25] și ale Curții Europene de Justiție din ultimii 2 ani[26].

Astfel, **recomandăm renunțarea la orice măsură generalizată de obligaţie de păstrare a datelor de trafic,** care au fost în mod constant declarate ca fiind contrare drepturilor fundamentale. Recomandăm revizuirea art. 132[11] limitând aplicabilitatea acestuia doar la interceptarea datelor de conţinut, aplicată în condiţii şi limite similare interceptărilor comunicațiilor electronice.

6. Art. III p. 8 al proiectului nr. 161, care prevede introducerea în Art. 133 Codul Penal, în titlu, după cuvintele „trimiterilor poştale" cuvintele „şi a comunicărilor electronice"; *la alineatul (1), după cuvintele „trimiterile poştale" se introduce textul „şi/sau comunicările electronice"; la alineatul (2), după cuvintele „trimiteri poştale" se introduce textul „şi/sau comunicări electronice", iar după cuvîntul „fax" se introduc textul „, mesageria textuală prin sisteme informatice în afara serviciilor de telefonie"; la alineatul (3), după cuvintele „trimiterilor poştale" se introduce textul „şi/sau comunicărilor electronice", după cuvintele „instituţiei poştale" se introduce textul „sau, după caz, prestatorului de servicii de poştă electronică sau mesagerie textuală", iar după cuvintele „trimiteri poştale" se introduce textul „şi/sau comunicări electronice"; la alineatul (4), după cuvintele „instituţiei poştale" se introduce textul „sau, după caz, prestatorului de servicii de poştă electronică sau mesagerie textuală"; la alineatul (5), după cuvintele „instituţiei poştale" se introduce textul „sau, după caz, prestatorul de servicii de poştă electronică sau mesagerie textuală"; la alineatul (6), după cuvintele „trimiterilor poştale" se introduce textul „şi/sau comunicărilor electronice".*

---

[24] Art. 132[9] CPP prevede efectuarea şi certificarea interceptării şi înregistrării comunicărilor de către organul de urmărire penală sau de către ofiţerul de investigaţii, cu autorizarea judecătorului de instrucție.

[25] Ne referim la deciziile curtilor din Germania, România, Cehia sau Slovacia pe problema datelor de trafic – deja citate la fn. 8. O lista comprehensiva a situației din mai multe state membre poate fi găsită aici - http://wiki.vorratsdatenspeicherung.de/Transposition.

[26] Spre exemplu, hotărârea CJUE în cauza C-362/14 Maximillian Schrems/Data Protection Commissioner http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117ro.pdf; Hotărârea CJUE din 8 aprilie 2014 în cauzele conexate C-293-12 şi C-594-12 *Digital Rights Ireland* *http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=RO*.

În opinia noastră reținerea, cercetarea, predarea, percheziționarea sau ridicarea trimiterilor poștale ar trebui să fie reglementate în mod distinct fața de orice formă de comunicare electronică, având în vedere natura tehnică diferită dintre ele, dar și natura distinctă a tipologiei de servicii:

- serviciile poștale sunt strict reglementate iar furnizorul are control asupra întregului proces;
- serviciile de comunicații electronice sunt reglementate, dar în unele cazuri furnizorul nu are control asupra serviciilor la care permite accesul, în funcție dacă este furnizor de telefonie, televiziune prin cablu sau furnizori de servicii Internet;
- serviciile online (sau servicii ale societății informaționale) – cum ar fi, din textul de mai sus, serviciile de "*mesagerie textuală prin sisteme informatice în afara serviciilor de telefonie" sau "poșta electronică"* - care sunt relativ puțin reglementate, pot fi centralizate sau descentralizate, criptate sau nu, cu cheie de criptare pe server sau cu criptat de la un capăt la altul al rețelei (end-to-end)[27].

În acest context ar trebui să și subliniem că folosirea unor termeni care țin de specificitatea unei comunicații (gen fax, poșta electronică sau mesagerie textuală) nu țin cont de principiul neutralității tehnologice și au toate șansele să sfârșească la fel ca "telegraful" în textul din zilele noastre. De aceea considerăm că, comunicațiile electronice urmează a fi reglementate în articole separate de cele poștale, iar în privința comunicațiilor electronice ar trebui să se opereze cu noțiuni generice și concepte cadru, cum ar fi:

- interceptarea comunicațiilor electronice, indiferent dacă este voce sau text, dacă este poștă electronică, chat, mesagerie textuală sau mesagerie video; și
- accesul la datele de trafic, care nu cuprind conținutul comunicării și care poate fi mai puțin intruziv.

De asemenea, și tipul de obligații ar trebui sa fie direct legat de categoria de servicii prestată. În același timp, avertizăm asupra posibilității supra-reglementării, dar și a reglementării imposibil de aplicat (vezi punctele VI și VII secțiunea A de mai sus), ceea ce ar duce în final la nerezolvarea problemelor de fond legate de criminalitatea informatică.

Respectiv, recomandăm excluderea art. III p. 8 din proiectul nr. 161, care prevede includerea sintagmei *„și a comunicărilor electronic*e" la art. 133 Codul de procedură penală, făcând o confuzie periculoasă între comunicările electronice și comunicările poștale și modurile de acces la acestea.

7. Art. VI p. 1 din proiectul nr. 161, care prevede că dispoziția articolului 90 a Codului Contravențional[28] se completează în final cu textul „,sau accesarea acestora cu bună știință în locuri publice".

Materialele de pornografie adultă intră în majoritatea statelor din Europa în categoria conținutului legal, dar posibil dăunător pentru minori (*harmful content*). În acest context accentul ar trebui să se pună pe măsuri nelegislative care să nu permită accesarea acestui tip de conținut de către copii, dar și măsuri de educație eficiente și nu pe limitări legislative pe acest tip de conținut, care oricum sunt iluzorii în cazul Internetului. Copii pot sa aibă acces accidental la conținut pornografic în orice loc unde există acces la Internet – indiferent dacă este locul public sau nu. De aceea soluția trebuie corelată în mod direct cu problema.

Relevante în acest sens sunt următoarele materiale:

---

[27] Pentru detalii a se vedea Bogdan Manolea, Principiul end-to-end al Internetului si implicațiile sale asupra dreptului - http://legi-internet.ro/blogs/index.php/principiul_end_to_end_al_internetului_si.

[28] Dispoziția actuală a art. 90 a Codului Contravențional prevede următoarele: „Producerea, comercializarea, difuzarea sau păstrarea produselor pornografice pentru a fi comercializate ori difuzate".

- Consiliul Europei - Protecting children against harmful content (2013) - https://edoc.coe.int/en/children-and-the-internet/5779-protecting-children-against-harmful-content.html
- Rapoartele și recomandările principalului proiect de cercetare din UE pe acest subiect – EU Kids online http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Respectiv, recomandăm renunțarea la introducerea sancțiunilor pentru accesarea materialelor de pornografice adultă cu bună știință de către adulți în locuri publice și, respectiv, excluderea Art. VI p. 1 din proiectul de lege nr. 161.

8. Art. VI p. 2 din proiectul nr. 161, care prevede completarea Codului Contravențional cu articolul 247[1] cu următorul cuprins: „Articolul 247[1]. Încălcarea legislației cu privire la prevenirea și combaterea criminalității informatice.
Încălcarea legislației cu privire la prevenirea și combaterea criminalității informatice de către furnizorii de servicii de comunicații electronice, indiferent de tipul de proprietate și forma juridică de organizare, manifestată prin:…”.

Mai jos ne vom referi la câteva acțiuni incluse în art. 247[1] Codul Contravențional care sunt problematice și care urmează fie a fi excluse, fie a fi reformulate.

I.1. „a) neîndeplinirea obligației de ținere a evidenței utilizatorilor de servicii;”

Obligație inclusă în lit. a) art. 247[1] Codul Contravențional este extrem de vagă și neclară în condițiile în care nu este suficient de clar despre ce tip de servicii discutăm. De asemenea, această obligație pare că pornește de la premisa că nu există un drept de a comunica anonim (a se vedea pct. VI din secțiunea A din opinie pentru detalii).

Respectiv, recomandăm renunțarea la această prevedere sau clarificarea ei pentru anumite categorii de furnizori de servicii, astfel încât și aceștia să își poată adapta comportamentul pentru a se conforma legii.

I.2. „b) necomunicarea către autoritățile competente despre accesul ilegal la informația din sistemul informatic, despre tentativele de introducere a unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informației ori a regulilor de protecție a sistemului informatic prevăzute în conformitate cu statutul informației sau cu gradul ei de protecție, dacă acestea au contribuit la însușirea, la denaturarea sau la distrugerea informației ori au provocat alte urmări grave, perturbarea funcționării sistemelor informatice, alte incidente de securitate informatică cu impact semnificativ;”

În lumea întreagă există o reticență de raportare a infracțiunilor informatice către autoritățile penale competente a cărei motivație rezidă în principal în contradicția dintre faptul că procesul penal va ajunge într-o fază publică și nevoia de protecție a datelor sau imaginii firmei sau persoanei respective. În acest sens, autoritățile ar trebui să se axeze mai mult pe încurajarea colaborării și nu prin sancționarea ne-colaborării.

În același timp ar trebui sa fie explicitate nivelul de la care această raportare devine obligatorie, pentru a nu lăsa această decizie la latitudinea subiectivă a celui afectat (ne referim în special la termenii de “*alte urmări grave; “perturbarea funcționării sistemelor informatice”* sau *“alte incidente de securitate informatică cu impact semnificativ”*.)

Astfel recomandăm reconsiderarea sancţiunii de ne-colaborare, cu prevederea colaborării voluntare sau limitarea posibilităţii de sancţionare pentru ne-raportare la un cerc mai restrâns de subiecţi şi clarificarea termenilor folosiţi în art. 247[1] lit. b) Codul Contravenţional (termenii neclari: „alte urmări grave"; „perturbarea sistemelor informatice", „alte incidente de securitate informatică cu impact semnificativ").

I.3. „f) neasigurarea păstrării datelor referitoare la trafic, în condiţiile stabilite de lege, pentru identificarea furnizorilor de servicii, utilizatorilor de servicii şi a canalului prin al cărui intermediu comunicaţia a fost transmisă;"

Această obligație, așa cum este formulată în proiectul nr. 161, reprezintă de fapt o obligație generalizată de păstrare a datelor de trafic, fiind astfel măsură de supraveghere generalizată și creează premise pentru violarea dreptului la viața privată (a se vedea contextul explicat detaliat la pct. IV secțiunea A din opinie, mai sus).

În contextul deciziilor CJUE Digital Rights Ireland și Schrems, ca și a deciziilor Curților constituționale menționate în cap IV mai sus și punctul 5 de mai sus, recomandăm renunțarea la această prevedere de supraveghere generalizată.

I.4. „g) neîndeplinirea obligaţiei de sistare, folosind metodele şi mijloacele tehnice din posesie, în condiţiile stabilite de lege, a accesului la toate adresele IP pe care sînt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, conţin informaţii ce fac propagandă războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă, conţin sau difuzează instrucţiuni privind modul de comitere a infracţiunilor,"

Această obligație ar putea încălca dreptul la libertate de exprimare, dar și la cel de viață privată, în funcție de modalitatea tehnică de implementare - vezi contextul explicat la pct. V secțiunea A din opinie.

De altfel sintagma de „sistare a accesului la toate adresele IP pe care sunt amplasate pagini web", este incorectă, inclusiv din punct de vedere tehnic – de la faptul că termenul corect este cel de blocare, la faptul că o pagina web sau mai multe pagini web pot fi găzduite la aceeași adresă IP până la faptul că în actualul context de dezvoltare informațională, în care datele sunt găzduite de intermediari – gen servicii de cloud computing sau de Content Distribution Network (CDN)[29] - accesul la o adresă IP indicată s-ar putea să nu blocheze deloc conținutul dorit și în schimb să blocheze un conținut nedorit.

Mai mult, sintagma "informații ce îndeamnă la ură sau discriminare națională, rasială ori religioasă" este extrem de generică – pe baza acesteia ar trebui să se blocheze accesul la Facebook, YouTube și Twitter care cu siguranță conțin astfel de informații.

Inclusiv sintagma "conţin sau difuzează instrucţiuni privind modul de comitere al infracţiunilor " este extrem de vagă și periculoasă. Pentru a da un singur exemplu banal: doar pe YouTube există 76 000 de filme[30] care vă arată cum deschideți o ușă fără a avea o cheie.

[29] A se vedea explicarea conceptului si o lista de furnizori majori la https://en.wikipedia.org/wiki/Content_delivery_network

[30] A se vedea spre exemplu aici : https://www.youtube.com/results?search_query=how+to+open+a+locked+door+without+a+key

La fel de neclar este cine stabilește că o adresă IP trebuie blocată, ce posibilități de apel există, ca și alte detalii practice care fac ca o astfel de măsură mai mult să creeze premise de cenzură decât să aibă vreun efect pozitiv.

În contextul acestor termeni vagi, dar și a deciziilor CtEDO *Ahmet Yıldırım c. Turciei* și *Cengiz și Ceilalți c. Turciei*, și a celorlalte argumente menționate în cap V mai sus, recomandăm excluderea din proiectul nr. 161 a obligației de "sistare a accesului la toate adresele IP pe care sînt amplasate pagini web", propuse în lit. g) a Codului Contravențional.

9. Art. VII al proiectului nr. 161 prevede o serie de modificări la Legea nr. 20 din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice. Mai jos ne vom referi la cele mai problematice, cu recomandările de rigoare.

În contextul legii privind criminalitatea informatică, pentru a rezolva problemele de criminalitate informatică, credem că ar fi necesară o focalizare a activităților pe înțelegerea fenomenului de ansamblu, inclusiv din punct de vedere sociologic sau criminologic. În acest sens sunt recomandate mai degrabă activitățile de cooperare internațională inter-statală, dar și de dezvoltare a resurselor umane necesare în a se axa pe problematica criminalității informatice, decât introducerea unor prevederi vagi și problematice.

9.1. Art. VII p. 4. al proiectului nr. 161 prevede că „Articolul 5 se completează cu alineatul (2) cu următorul cuprins: „(2) Furnizorii de servicii, organizaţiile neguvernamentale, reprezentanţii societăţii civile şi orice altă persoană sînt încurajaţi să transmită în adresa Inspectoratului General al Poliţiei şi Procuraturii Generale orice informaţii, ce le devin cunoscute, cu privire la persoane fizice şi/sau juridice care distribuie, difuzează, importă sau exportă imagini sau alte reprezentări ale unui sau mai mulţi copii implicaţi în activităţi sexuale, precum şi cu privire la abuzuri sexuale comise faţă de un copil prin utilizarea comunicaţiilor electronice."

Deși aceasta este o direcție susținută în toată lumea în special pentru raportarea materialelor de pornografie infantilă distribuite prin rețele informatice, este foarte probabil să nu fie eficace în măsura în care simpla deținere este considerată o infracțiune.

În acest sens recomandăm dezincriminarea „simplei deţineri" pentru a putea permite raportarea de conținut ilegal către autoritățile competente. Acesta este și scopul limitării din art. 9 Alin (4) din Convenția de la Budapesta care permite statelor membre să nu incrimineze „simpla posesie". De altfel, nu toate statele semnatare ale Convenției de la Budapesta au incriminată o astfel de infracțiune.

9.2. Art. VII p. 5 al proiectului nr. 161 prevede modificări la art. 6^1 al Legii nr. 20 şi anume: d) să comunice autorităţilor competente imediat, dar nu mai târziu de 24 de ore de la momentul depistării, informaţiile despre accesul ilegal la datele din propriul sistem informatic, despre tentativele de introducere ale unor programe ilegale, despre încălcarea de către persoane responsabile a regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic prevăzute în conformitate cu statutul informaţiei sau cu gradul ei de protecţie, dacă acestea au contribuit la însuşirea, denaturarea sau distrugerea informaţiei ori au provocat alte urmări grave, perturbarea funcţionării sistemelor informatice, alte incidente de securitate informatică cu impact semnificativ."

După cum am menționat mai sus la analiza propunerii din proiect cu privire la art. 247^1 lit. b) Cod Contravențional, în lumea întreagă există o reticență de raportare a infracțiunilor informatice către autoritățile penale competente a cărei motivație rezidă în principal în contradicția dintre faptul că procesul penal va ajunge într-o fază publică și nevoia de protecție a datelor sau imaginii firmei sau persoanei respective. În acest sens,

autoritățile ar trebui să se axeze mai mult pe încurajarea colaborării și nu prin sancționarea ne-colaborării.[31]

Eventual se poate cere raportarea doar pentru categorii limitate de infracțiuni unde pericolul social și identificarea cazurilor ce trebuie raportate este clară pentru toți subiecții legii – de ex. Infracțiunile asupra sistemelor informatice aparținând infrastructurilor critice ale statului (dacă acestea sunt definite în alte acte normative) sau infracțiunile asupra sistemelor informatice aparținând băncilor.

În același timp ar trebui sa fie explicitat nivelul de la care această raportare devine obligatorie, pentru a nu lăsa această decizie la latitudinea subiectivă a celui afectat (ne referim în special la termenii de "*alte urmări grave; "perturbarea funcționării sistemelor informatice"* sau *"alte incidente de securitate informatică cu impact semnificativ"*.). Subiectul este strâns legat de alte notificări similare, dar cu consecințe mai mici pentru operatorii privați (vezi notificări pentru încălcări de securitate pe zona de protecției datelor cu caracter personal) unde s-au identificat multe bune si rele practici pe acest subiect.[32]

<u>În concluzie, recomandăm reconsiderarea și rescrierea acestui articol, având în vedere obiectivul de a încuraja raportarea de infracțiuni în mod voluntar.</u>

Ar trebui explicitat și ce înseamnă autorități competente și care este scopul raportării, acesta putând fi văzut din 3 zone diferite:

- raportarea către organele de urmărire penală pentru identificarea și pedepsirea vinovaților,
- raportarea către organe de securitatea informației (de ex. o unitate de tip CERT), pentru oprirea sau reducerea efectelor încălcării securității informatice (vezi propunerea de directivă pentru securitatea rețelelor și sistemelor de informații (Directiva NIS)[33])
- raportarea către autoritățile din domeniul protecției datelor cu caracter personal, în scopul eventualei informări a persoanelor vizate (vezi Regulamentul UE privind protecția datelor cu caracter personal[34] – de implementat în toate statele membre ale UE din 2018).

<u>9.3. Art. VII p. 6 al proiectului nr. 161 prevede modificări la art. 7 al Legii nr. 20 și anume: alineatul (1): litera a) se completează în final cu textul „, iar în cazul serviciilor anonime preplătite – data și ora primei activări a serviciului"; la litera b), textul „datele despre traficul informatic, inclusiv" se substituie cu textul „, prevăzute la art. 4 alin. (1),", iar cuvintele „delicte informatice" se substituie cu cuvintele „incidente de securitate informatică cu impact semnificativ";</u>

Aceste date (Data și ora primei activări a serviciului anonim, datele despre traficul informativ și incidente de securitate informatică cu impact semnificativ) fac parte din datele de trafic colectate în mod generalizat și nejustificat (a se vedea comentariile de mai sus cu privire la aceste aspecte de păstrare a datelor de trafic cap IV secțiunea A sin opinie).

<u>În contextul deciziilor CJUE Digital Rights Ireland și Schrems, cât și a deciziilor Curților Constituționale menționate în cap IV, recomandăm renunțarea la această prevedere de supraveghere generalizată.</u>

---

31 A se vedea și Best practices de la Ministerul Justiției din SUA ca un exemplu în acest sens - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

32 A se vedea de exemplu raportul ENISA - Data breach notifications in the EU https://www.enisa.europa.eu/publications/dbn

33 A se vedea propunerea aici https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive.

34 Text integral disponibil la http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC

9.4. Art. VII p. 6 al proiectului nr. 161 prevede modificări la art. 7 al Legii nr. 20 și anume: alineatul (1): la litera c), cuvântul „imediată" se substituie cu cuvântul „rapidă", după cuvintele „traficul informatic" se introduce textul „indicate în solicitarea respectivă", iar textul „120 de zile calendaristice" se substituie cu textul „180 de zile calendaristice";

Orice extindere a legislației care aduce atingere drepturilor fundamentale trebuie însoțită de o analiză asupra necesității ingerinței într-o societate democratică. În acest caz prelungirea termenului cu 2 luni nu este justificată în niciun mod.

Mai mult, reamintim că directiva europeană 2006/24/EC care prevedea un termen de 6 luni a fost considerată excesivă și că încalcă drepturile fundamentele ale cetățenilor UE. De altfel în contextul deciziilor CJUE Digital Rights Ireland și Schrems, cât și a deciziilor Curților Constituționale menționate în cap IV, acest subiect ar trebui revizuit în întregime.

Respectiv, recomandăm renunțarea completă la orice măsură de păstrare a datelor de trafic, deci inclusiv la acest amendament.

9.5. Art. VII p. 6 al proiectului nr. 161 prevede modificări la art. 7 al Legii nr. 20 și anume: alineatul (1) la litera f), textul „monitorizarea, supravegherea şi" se exclude, iar textul „„pe o perioadă de 180 de zile calendaristice" se substituie cu textul „în reţeaua de telefonie fixă şi de telefonie mobilă pe o perioadă de un an, iar a celor referitoare la trafic în Internet şi telefonie prin Internet – pe o perioadă de 6 luni";

Orice extindere a legislației care aduce atingere drepturilor fundamentale trebuie însoțită de o analiză asupra necesității ingerinței într-o societate democratică. În acest caz prelungirea termenului nu este justificată în niciun mod.

Mai mult, reamintim că directiva europeană 2006/24/EC care prevedea un termen de 6 luni a fost considerată excesivă și că încalcă drepturile fundamentale ale cetățenilor UE. De altfel în contextul deciziilor CJUE Digital Rights Ireland și Schrems, cât și a deciziilor Curților constituționale menționate în cap IV, acest subiect ar trebui revizuit în întregime.

Respectiv, recomandăm renunțarea completă la orice măsură de păstrare a datelor de trafic, deci inclusiv la acest amendament.

9.6. Art. VII p. 6 al proiectului nr. 161 prevede modificări la art. 7 al Legii nr. 20 și anume: alineatul (1) „h) să sisteze, în condiţiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la toate adresele IP pe care sînt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, conţin informaţii ce fac propagandă războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă, conţin sau difuzează instrucţiuni privind modul de comitere a infracţiunilor" .

Obligațiile de „sistare a accesului" propuse prin art. 7 alin. (1) lit. h) ar putea încălca dreptul la libertatea de exprimare, dar și la cel la viață privată, în funcție de modalitatea tehnică de implementare. A se vedea și contextul detaliat la pct. V (blocarea adreselor IP) și comentariul de la pct. VIII.4 de mai sus.

Conform opiniei la actuala opinie, prezentată de Centrul pentru Combaterea Crimelor Informatice, în cadrul dezbaterilor proiectului de lege nr. 161 în Comisiile Parlamentare, s-a propus următoarea redacție a art. 7 alin. (1) lit. h): „h) să sisteze în condiţiile legii, folosind metodele şi mijloacele tehnice din posesie, accesul din propriul sistem informatic la paginile web pe care sînt amplasate pagini web, inclusiv cele găzduite de furnizorul respectiv, ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, conţin informaţii ce fac propaganda războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violență."

Art. 7 s-a completat cu alin. 3 cu următorul cuprins: „"(3) Sistarea accesului la paginile web, prevăzute la alin. (1) lit. h) din prezentul articol, se dispune de instanţă în cadrul cauzelor penale, în cazul în care furnizorul de servicii nu a eliminat din paginile web găzduite sau aflate sub controlul său informaţia respectivă la solicitarea organelor de drept sau dacă stabilirea datelor de contact ale acestui furnizor de servicii nu a fost posibilă. Sistarea accesului la paginile web ce conţin pornografie infantilă, promovează abuzul sexual sau exploatarea sexuală a copiilor, ce nu sunt găzduite de furnizorul respectiv, se dispune de organele de drept conform Listei elaborate de Organizaţia Internaţională a Poliţiei Criminale (INTERPOL "Worst of"-list), pusă la dispoziţia furnizorului de servicii."

Din păcate nici textul propus către Parlament nu este în măsură a clarifica problema, menționând în mod confuz în același articol termeni de furnizor de servicii care are pagini web găzduite și sistarea accesului la paginile web. Furnizor de servicii este atât un furnizorul de acces la Internet, cât și un furnizor de găzduire, dar fiecare are tipuri de responsabilități diferite. Mai mult în acea variantă – referința la Lista „Worst-of" a Interpol – dovedește că încă nu s-au analizat suficient opțiunile tehnice. Astfel lista respectivă blochează domenii, și nu pagini web și nici adrese IP, ce ridică un set diferit de probleme.

De asemenea în același articol sunt întâlnite situații diametral opuse - în primul paragraf blocarea se dispune de către instanță, dar în al doilea se dispune de „organele de drept" conform unei liste internaționale, care excede cadrul juridic național (e vorba de un „soft law").

În contextul textului extrem de vag şi a deciziilor CEDO Ahmet Yıldırım v. Turcia şi Cengiz şi Ceilalți v. Turcia, nr. 48226/10 şi 14027/11, 1 decembrie 2015, cât şi a celorlalte argumente menționate în pct. V al opiniei, **recomandăm excluderea din Legea nr. 20 a prevederii care permite și solicită "sistarea accesului". În schimb sugerăm obligaţii clare pentru furnizorii care găzduiesc aceasta informaţie şi care refuză să o şteargă şi să identifice persoanele care au publicat acel material ilegal.**

9.7. Art. VII p. 7 al proiectului nr. 161 prevede modificări la art. 10 al Legii nr. 20 şi anume se propune modificarea alin. (5) după cum urmează: „(5) În cazul în care, în timpul executării unei solicitări de conservare a datelor referitoare la trafic, autoritatea competentă din Republica Moldova descoperă că un furnizor de servicii a participat într-un alt stat la transmiterea acestei comunicări, aceasta va dezvălui rapid autorităţii competente străine solicitante o cantitate suficientă de date referitoare la trafic, pentru identificarea acestui furnizor de servicii şi a canalului prin care comunicarea a fost transmisă."

Textul ar putea fi interpretat în sensul că un furnizor de servicii din Republica Moldova poate dezvălui unei autorități publice străine informații care pot fi de natură personală (datele de trafic) fără vreo garanție procesuală în acest caz. Considerăm că formularea ar trebui să fie clarificată în contextul unei explicații a nevoii de adăugire a acestui articol.

Recomandarea ar fi în primul rând de specificare expresă a nevoii de a introduce acest articol specific în nota proiectului nr. 161 şi revizuirea textului articolului pentru a specifica că informaţiile care pot fi transmise în

străinătate nu pot conţine date personale, care ar putea fi eventual dezvăluite doar cu autorizaţia judecătorului, în condiţiile prevăzute de legislaţia Republicii Moldova.