Informare pentru organismele naționale de control al serviciilor de informații, despre implicațiile schimbului de informații între state

PRIVACY INTERNATIONAL

Septembrie 2017

I. Introducere

Controlul efectiv al schimbului de informații este una dintre garanțiile fundamentale împotriva intruziunii statului în viața privată. Din păcate, există o lipsă alarmantă de control efectiv al supravegherii secrete, într-o serie de țări. Înaltul Comisar al Națiunilor Unite pentru Drepturile Omului observă:

> „Lipsa de control efectiv a contribuit la o lipsă de responsabilitate pentru intruziuni arbitrare și ilegale în viața privată în mediul digital. Mai ales măsurile de protecție interne, fără monitorizare externă independentă, s-au dovedit ineficiente împotriva metodelor ilegale sau arbitrare de supraveghere. Deși aceste măsuri de protecție pot avea o serie de forme, implicarea tuturor puterilor în stat în controlul programelor de supraveghere, cât și existența unei agenții civile de control, sunt esențiale în asigurarea protecției efective a legii."[1]

Un exemplu aparte de lipsă de măsuri eficiente s-a observat la înțelegerile bilaterale și multilaterale privind schimbul de informații. Privacy Internațional descrie:

- Înțelegerile privind schimbul de informații
- Cadrele legale internaționale și locale privind schimbul de informații
- Implicațiile internaționale ale schimbului de informații în privința drepturilor omului

Privacy International încheie cu o serie de recomandări pentru organismele naționale de control al serviciilor de informații. Recomandările îndeamnă aceste organisme la sporirea transparenței înțelegerilor privind schimbul de informații la care statele respective sunt parte și la examinarea mai minuțioasă a acestor înțelegeri, inclusiv examinarea conformității acestora cu legislația internațională și națională.

II. Schimbul de informații

Înțelegerile privind schimbul de informații acoperă o serie de posibile activități între state, inclusiv, *inter alia*, schimbul de informații, cooperarea operațională, găzduirea de obiective și echipament, antrenament și consolidarea capacităților și susținere tehnică și financiară.[2] În fiecare dintre aceste categorii există o gamă largă de interacțiuni posibile. Schimbul de informații, de exemplu, poate merge de la înțelegeri *ad hoc* privind schimbul de informări cu un anumit scop, sub rezerva unor cereri și aprobări bine definite, până la schimbul automatizat de date de interceptare brute sau gestionarea comună a unor baze de date.[3]

---

1 Raport al Biroului Înaltului Comisar ONU pentru Drepturile Omului, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/27/37, par. 37 (30 June 2014).

2 Ca lectură suplimentară, *vezi* Hans Born et al., *Making International Intelligence Cooperation Accountable*, pp. 18-25 (2015).

3 Pentru o analiză a practicilor de schimb de informații, în special în contextul relației de înaltă integrare dintre serviciilor de informații ale Statelor Unite ale Americii și ale Marii Britanii, *vezi* Witness Statement of Eric King, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and the Government*

Una dintre cele mai des menționate înțelegeri privind schimbul de informații este alianța Five Eyes (Cinci Ochi) – o înțelegere globală de supraveghere formată din National Security Agency (NSA) din SUA, Government Communications Headquarters (GCHQ) din Marea Britanie, Communications Security Establishment Canada (CSEC), Australian Signals Directorate (ASD) și Government Communications Security Bureau (GCSB) din Noua Zeelandă. Deși este veche de 70 de ani, se știu foarte puține despre această alianță și înțelegerea/înțelegerile care o guvernează.[4] Chiar și mai puține se știu despre alte parteneriate de supraveghere care au evoluat pornind de la Five Eyes, cum ar fi 9-Eyes (Five Eyes + Danemarca, Franța, Olanda și Norvegia), 14-Eyes (9-Eyes + Belgia, Germania, Italia, Spania și Suedia) și 43-Eyes (14-Eyes + membrii International Security Assistance Forces din Afganistan, din 2010)[5].

Mai există și alte înțelegeri bilaterale și multilaterale privind schimbul de informații care acoperă alte zone geografice. De exemplu:

- Clubul de la Berna este o înțelegere privind schimbul de informații între serviciile de informații ale membrilor Uniunii Europene. European Union Agency for Law Enforcement Cooperation (EUROPOL) este instituția de aplicare a legii a UE și promovează schimbul de informații între membrii UE.[6]
- Africa-Frontex Intelligence Community (AFIC) este o înțelegere privind schimbul de informații între țările europene și cele africane, în domeniul siguranței frontierelor.[7]
- Great Lakes Regions Intelligence Fusion Centre facilitează schimbul de informații între 11 țări din acea regiune.[8]
- Shanghai Cooperation Organization (SCO) este o înțelegere privind schimbul de informații între China, Rusia, Kazakhstan, Kârgâzstan, Tadjikistan și Uzbekistan.[9]

Communication Headquarters, Investigatory Powers Tribunal, IPT/13/92/CH, paras. 70-90 (8 June 2014), available at www.privacyinternational.org/sites/default/files/Eric%20King%20witness%20statement_0.pdf.

4 Pentru un rezumat a ceea ce știm despre alianța Five Eyes, *vezi* Privacy International, *Eyes Wide Open*, 26 Nov. 2013, disponibil la https://www.privacyinternational.org/node/301.

5 Ca lectură suplimentară pe tema 43-Eyes, vezi *Five Eyes, 9-Eyes, and Many More*, Electrospaces.net, 15 Nov. 2013, http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html. Lista completă a statelor 43-Eyes este următoarea: SUA, Marea Britanie, Canada, Australia, New Zeelandă, Danemarca, Franța, Olanda, Norvegia, Belgia, Germania, Italia, Spania, Suedia, Albania, Armenia, Austria, Azerbaidjan, Bosnia și Herțegovina, Bulgaria, Croația, Cehia, Estonia, Finlanda, Georgia, Grecia, Ungaria, Islanda, Irlanda, Letonia, Lituania, Luxemburg, Macedonia, Muntenegru, Polonia, Portugalia, România, Slovacia, Slovenia, Coreea de Sud, Elveția, Turcia și Ucraina. Privacy International admite că aceste alianțe se poate să se fi modificat odată cu trecerea timpului. Lipsa generală de claritate din jurul înțelegerilor privind schimburile de date face dificilă confirmarea stării prezente de fapt.

6 James Igoe Walsh, The International Politics of Intelligence Sharing, 88-110 (2010).

7 *Vezi în general*, Frontex Publishes Africa-Frontex Intelligence Community (AFIC) Report (6 Apr. 2017), disponibil la http://frontex.europa.eu/news/frontex-publishes-africa-frontex-intelligence-community-afic-report-acjRuQ.

8 Steven Addamah, *Central Africa: Great Lakes Countries Upgrade Intelligence Sharing Cooperation*, Medafrica Times, 26 June 2012, disponibil la http://medafricatimes.com/329-central-africa-great-lakes-countries-upgrade-intelligence-sharing-cooperation.html. Cele 11 țări sunt: Angola, Burundi, Republica Centrafricană, Congo, Republica Democrată Congo, Kenya, Rwanda, Sudan, Tanzania, Uganda și Zambia.

9 Eleanor Albert, Council on Foreign Relations, The Shanghai Cooperation Organization Backgrounder (14 Oct. 2015), disponibil la https://www.cfr.org/backgrounder/shanghai-cooperation-organization.

- Rusia, Irak, Iran și Siria au făcut o înțelegere privind schimbul de informații pentru a facilita cooperarea în combaterea Statului Islamic.[10]

III. Cadrele legale internaționale și locale privind schimbul de informații

Înțelegerile privind schimbul de informații sunt de obicei confidențiale și nu sunt supuse controlului public, de multe ori funcționând sub forma unor memorandumuri de înțelegere direct încheiate între ministerele sau agențiile relevante. Astfel de înțelegeri pot enunța în mod explicit că nu pot fi considerate instrumente obligatorii din punct de vedere juridic, conform legislației internaționale.[11] Din acest motiv, aceste înțelegeri pot eluda necesitatea ratificării, conform procedurilor constituționale și/sau a legilor naționale ale fiecărui stat partener, cât și înregistrarea la Secretariatul ONU, în concordanță cu Articolul 102 al Cartei ONU.

Mai mult decât atât, majoritatea țărilor din lume nu au legislația necesară pentru controlul schimbului de informații. Multe țări au introdus abia în ultimele decade o bază legislativă pentru activitățile serviciilor de informații. Această bază legislativă ar trebui să acopere înțelegerile privind schimbul de informații pentru a le oferi legitimitate din punct de vedere democratic. În lipsa acesteia, aceste agenții pot folosi aceste înțelegeri pentru a eluda legislația internațională și națională privind activitățile de strângere de informații. Raportorul special ONU pentru Antiterorism a spus următoarele:

> „Absența legilor care să reglementeze schimbul de informații între state a lăsat deschisă calea pentru înțelegeri bilaterale și multilaterale ale serviciilor de informații, care nu sunt sub controlul niciunei autorități independente. Informații privind comunicațiile persoanelor pot fi partajate cu servicii străine de informații, fără nici un cadru legal accesibil public și fără (nicio) protecție... Astfel de practici fac funcționarea regimului de supraveghere imprevizibilă pentru cei afectați de acesta și, prin urmare, incompatibilă cu articolul 17 al Convenției [Internaționale privind Drepturile Civile și Politice].”[12]

IV. Implicațiile internaționale ale schimbului de informații în domeniul drepturilor omului

---

10 J. Dana Stuster, *Russia, Iran, Iraq, and Syria to Share Intelligence on Islamic State*, Foreign Policy, 28 Sept. 2015, disponibil la http://foreignpolicy.com/2015/09/28/russia-iran-iraq-and-syria-to-share-intelligence-on-islamic-state/.

11 *Vezi, de exemplu*, Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons, disponibil la www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf (observați că „acest acord nu are scopul de a crea drepturi obligatorii legale și nu nu va fi considerat ca un acord internațional sau legal, conform legislației internaționale”). Această înțelegere a fost publicată prima dată de The Guardian, pe 11 septembrie 2013. *Vezi* Glenn Greenwald et al., *NSA Shares Raw Intelligence Including Americans' Data with Israel*, The Guardian, 11 Sept. 2013, disponibil la https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

12 Raport al Raportorului Special ONU pentru Promovarea și Protecția Drepturilor Omului și a Libertăților Fundamentale în Contextul Combaterii Terorismului, U.N. Doc. A/69/397, para. 44 (23 Sept. 2014).

Articolul 17 al Convenției Internaționale privind Drepturile Civile și Politice protejează dreptul la viața privată. Comisia ONU pentru Drepturile Omului a afirmat în mod repetat, ca urmare a analizei practicilor privind schimbul de informații ale anumitor state membre, că legile și politicile care reglementează astfel de schimburi trebuie să fie în deplină conformitate cu obligațiile stipulate de Convenție. Comisia a punctat în mod special nevoia de respectare a Articolului 17, „inclusiv a principiilor de legalitate, proporționalitate și necesitate", cât și nevoia de a introduce „mecanisme efective și independente de control al schimbului de date personale de către serviciile de informații."[13]

Curtea Europeană pentru Drepturile Omului și-a exprimat îngrijorarea în legătură cu practica schimbului de informații și nevoia de a avea un control mai bun al acesteia:

> „Practica din ce în ce mai răspândită a statelor de a transfera și schimba informații obținute prin metode secrete de supraveghere – o practică a cărei utilitate în combaterea terorismului internațional, din nou, nu este în discuție și care privește atât schimburile între Statele Membre ale Consiliului Europei cât și cu alte jurisdicții – este un alt factor care necesită o atenție specială, în contextul unei supravegheri externe și a unor măsuri rectificative.[14]

Intruziunea în viața privată creată de schimbul de informații este echivalentă cu cea creată de supravegherea directă. Așa cum supravegherea desfășurată de stat trebuie să fie transparentă și să fie supusă unor cerințe de protecție și control, tot astfel trebuie să fie și înțelegerile privind schimburile de informații. Schimburile de informații netransparente, nestingherite și pentru care nu trebuie dat seamă nimănui amenință fundamentul cadrului legal al drepturilor omului și al statului de drept. În spcial, Privacy Internațional subliniază trei aspecte îngrijorătoare:[15]

1. Schimburile de informații pot duce la o situație de tip „ușă rotativă", în care statele eludează constrângerile internaționale și naționale în privința supravegherii directe, bazându-se pe parteneri pentru a obține și transmite informații. Un exemplu obișnuit de constrângere sunt restricțiile naționale privind abilitatea statului de a desfășura activități de supraveghere asupra propriilor cetățeni.[16] Nu este clar, de exemplu, cum

---

13 *Vezi* Concluding Observations on the Seventh Periodic Report of Sweden, U.N. Human Rights Committee, U.N. Doc. CCPR/C/SWE/CO/7, paras. 36-37 (28 Apr. 2016); Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, U.N. Human Rights Committee, U.N. Doc. CCPR/C/GBR/CO/7, para. 24 (17 Aug. 2015); Concluding Observations on the Sixth Periodic Report of Canada, U.N. Human Rights Committee, U.N. Doc CCPR/C/CAN/CO/6, para. 10 (13 Aug. 2015).

14 *Vezi* Szabó and Vissy v. Hungary, App. No. 37138/14, Curtea Europeană a Drepturilor Omului, Judgment, par. 78 (12 ian. 2016).

15 Pentru o listă mai detaliată de potențiale pericole ale schimbului de informații, *vezi* Born, *supra* note 2, la pp. 40-59.

16 *Vezi* Craig Forcese, *The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing*, *in* International Intelligence Cooperation and Accountability, Pre-Conference Draft Paper, Conference on Intelligence Sharing, seponsorizată de Comisisa Parlamentară de

această constrângere s-ar mai putea aplica în mod efectiv când un stat accesează sau primește date obținute en-gros de un alt stat. Statele ar mai putea, de asemenea, folosi în mod explicit înțelegeri privind schimbul de informații pentru a obține informații pe care altfel nu ar avea cum să le obțină prin supraveghere directă, cum ar fi informații privind propriii cetățeni.

2. Statele ar putea comunica informații cu state cunoscute pentru violări ale legislației internaționale privind drepturile omului. Astfel de schimb de informații pune în primejdie persoanele din aceste state în mod special. Aceste state ar putea, de exemplu, folosi informațiile primite pentru a persecuta minorități, imigranți, apărători ai drepturilor omului, dizidenți și jurnaliști.[17]

3. Schimbul de informații poate slăbi răspunderea în general. Agențiile sunt stimulate să nu întrebe de sursele și metodele folosite pentru obținerea unei informații pentru a se putea asigură că pot nega („plausible deniability") că știu de unde au obținut respectiva informație. Și chiar dacă ar fi să investigheze în privința surselor și metodelor, afirmațiile agenției sunt dificil de susținut în practică.[18] Mecanismele de control al activității de informații de multe ori sunt abilitate doar în privința activităților agențiilor naționale. Mai mult decât atât, multe înțelegeri privind schimburile de informații interzic dezvăluirea informațiilor comunicate către terți, ceea ce înseamnă inclusiv către mecanismele de control.[19]

Pentru a aborda aceste probleme, statele trebuie să stabilească, prin legislație primară, cadre legale accesibile public care guvernează schimburile de informații și care să stipuleze că:

- Înțelegerile privind schimbul de informații trebuie să fie înțelegeri obligatorii din punct de vedere juridic supuse procedurilor internaționale și naționale care guvernează astfel de înțelegeri;

Supraveghere a Informațiilor din Norvegia, pp. 90-92 (5 Mar. 2009), disponibil la https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=1354022; Comisarul pentru Drepturile Omului, Consiliul Europei, Positions on Counter-Terrorism and Human Rights Protection, p. 11 (5 June 2015) (observând că "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards"). Ca lectură suplimentară, vezi European Commission for Democracy through Law (Venice Commission), Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies, Study No. 719/2013 CDL-AD(2015)006, para. 11 (7 Apr. 2015).

17 *Vezi*, *în general*, Raportul Raportorului Special asupra Promovării și Protecției Dreptului la Libertatea de Opinie și Exprimare, U.N. Doc. A/HRC/29/32, para. 59 (22 May 2015); Biroul Raportorului Special pentru Libertatea de Exprimare a Comisiei Inter-americane pentru Drepturile Omului, Libertate de Exprimare și Internet, par. 150 (31 Dec. 2013).

18 Ca lectură suplimentară, vezi Comisia Europeană pentru Democrație prin Drept (Comisia de la Veneția), Raport privind Controlul Democratic al Serviciilor de Supraveghere, Studiul No. 388/2006 CDL-AD(2007)016, par. 115-121 (11 June 2007).

19 Ca lectură suplimentară, vezi Adunarea Parlamentară a Consiliului Europei (PACE), Rezoluția privind Supravegherea în Masă 2045, par. 19.2 (21 apr. 2015).

- Circumstanțe în care serviciile de informații vor face schimb de informații și procedurile folosite pentru aceasta trebuie să fie clare, inclusiv limitarea acestor schimburi la situațiile în care aceasta este necesar și proporțional;
- Constrângerile internaționale și naționale – inclusiv garanții și control efectiv – care se aplică supravegherii directe de către stat trebuie să se aplice în mod egal și informațiilor obținute prin intermediul schimburilor de informații;
- Trebuie să existe obligații de verificare („due diligence") pentru statele care obțin și apoi comunică informații, cât și pentru cele care accesează sau primesc informații. Ambele state sunt responsabile pentru colectarea, stocarea, analiza, folosirea și diseminarea informației. Obligațiile de verificare ale statelor pot cuprinde următoarele:
    - Statele care obțin și apoi comunică informații trebuie să analizeze antecedentele privind drepturile omului ale agențiilor cărora le sunt comunicate respectivele informații, cu accent special pe evaluarea existenței unor protecții efective pentru viața privată și dacă acele informații vor putea fi folosite mai târziu pentru a facilita încălcări ale drepturilor omului;
    - Statele care accesează sau primesc informații trebuie să analizeze corectitudinea și verificabilitatea informațiilor înainte de a se baza pe acea informație.
- Trebuie ca mecanismele de control să-și exercite puterile în privința activităților de schimb de informații ale statului și să aibă autoritatea, resursele și accesul necesar pentru a verifica toate aspectele înțelegerilor privind schimbul de informații.

V. Recomandări pentru Organismele de Control

Privacy Internațional îndeamnă, în mod specific, organismele de control al serviciilor de informații, în măsura mandatelor lor, să:

- Publice cât mai multe informații cu putință în legătură cu felul și amploarea înțelegerilor privind schimbul de informații la care statul ia parte, cât și regulile care guvernează aceste înțelegeri;
- Analizeze legislația existentă și regulile care guvernează schimburile de informații, cu accent pe evaluarea conformității acestora cu legislația internațională și națională, inclusiv în privința respectării dreptului la viața privată și a celorlalte drepturi ale omului; și să
- Inițieze investigații independente în privința practicilor de schimb de date ale statelor lor și să facă publice rezultatelor acestor investigații.

Privacy Internațional poate furniza documentație suplimentară și suport pentru realizarea acestor obiective.