Supravegherea de către serviciile de informații: măsurile de protecție și căile de atac privind drepturile fundamentale în Uniunea Europeană

Rezumat

Articolul 7 din Carta drepturilor fundamentale a Uniunii Europene garantează tuturor persoanelor fizice din Uniunea Europeană (UE) respectarea vieții private și de familie, în timp ce articolul 8 garantează dreptul la protecția datelor cu caracter personal ale acestora. Articolul impune tratarea acestor date în mod corect, în scopurile precizate, și asigură oricărei persoane dreptul de acces la datele cu caracter personal care o privesc, precum și dreptul de a obține rectificarea acestora. De asemenea, articolul prevede faptul că respectarea acestui drept se supune controlului unei autorități independente. Articolul 47 garantează dreptul la o cale de atac eficientă, inclusiv la un proces echitabil, public și întrun termen rezonabil.

Când mass-media din întreaga lume a început să publice „Documentele Snowden" în iunie 2013, a ieșit la iveală existența unor programe de supraveghere globală extinsă folosite de serviciile de informații. Dezvăluirile făcute de Snowden nu au fost primele care au făcut aluzie la supravegherea pe scară largă a comunicațiilor pusă la punct ca o consecință a atacurilor de la 11 septembrie 2001. Amploarea acestor dezvăluiri rămâne însă fără precedent, putând afecta intimitatea persoanelor din întreaga lume. Supravegherea nu mai are ca obiect numai secretele de stat sau de afaceri, ci permite interceptarea comunicațiilor la o scară mai largă. Acest lucru încalcă atât dreptul la respectarea vieții private și de familie al persoanelor fizice, cât și dreptul la intimitate și protecția datelor – ambele drepturi fiind garantate la nivelul UE prin Carta drepturilor fundamentale a Uniunii Europene (carta). Ca atare, UE și statele sale membre au obligația de a le proteja, inclusiv în contextul supravegherii, și de a pune la dispoziția victimelor căi de atac pentru contestarea supravegherilor nelegitime.

„Această supraveghere în masă nediscriminatorie este în mod inerent disproporționată și constituie o încălcare nefondată a drepturilor garantate de articolele 7 și 8 din cartă."
[CJUE, C-362/14, *Maximillian Schrems împotriva Data protection Commissioner* (Comisarului pentru Protecția Datelor), Concluziile avocatului general, 23 septembrie 2015]

Dezvăluirile au atras un șir întreg de reacții. În comunitatea de informații, în special în rândul organelor specializate responsabile cu supravegherea serviciilor de informații, cercetările dedicate și rapoartele speciale privind dezvăluirile Snowden au analizat cu și mai mare atenție implicațiile acestora. Instituțiile UE au reacționat energic. Comisia Europeană, Consiliul Uniunii Europene și Parlamentul European au raportat cu privire la dezvăluiri, și-au exprimat îngrijorarea cu privire la programele de supraveghere în masă, au cerut clarificări din partea autorităților Statelor Unite și au lucrat la „restaurarea încrederii" în relațiile SUA-UE. Deși este prea devreme să evaluăm impactul complet al dezvăluirilor lui Snowden, cercetările post-Snowden din anumite state membre ale UE au concluzionat că este necesară reformarea cadrelor juridice naționale actuale. Acest lucru a fost subliniat încă o dată de Hotărârea din luna martie 2014 a Parlamentului European privind programul de supraveghere al Agenției Naționale de Securitate (NSA) a Statelor Unite, organele de supraveghere din diferite state membre și impactul acestora asupra drepturilor fundamentale ale cetățenilor UE și asupra cooperării transatlantice în domeniul justiției și afacerilor interne [2013/2188(INI), P7_TA (2014)0230], lansând un *Habeas Corpus Digital European*.

„Dezvăluirile lui Snowden ne-au dat ocazia de a reacționa. Sper că vom transforma aceste reacții în ceva pozitiv și care să dureze până în următorul mandat al acestui Parlament, o lege privind protecția datelor de care să putem fi mândri."
(Claude Moraes, MEP, Raportor în ancheta NSA a Parlamentului European, Comunicat de presă, 12 martie 2014)

Reprezentarea grafică a cadrelor juridice ale statelor membre ale UE referitoare la supraveghere

În luna aprilie 2014, Parlamentul European a solicitat Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA) „să facă o cercetare amănunțită a protecției drepturilor fundamentale în contextul supravegherii". FRA s-a conformat, făcând reprezentarea grafică a cadrelor juridice ale celor 28 de state membre ale UE referitoare la supraveghere și furnizând o prezentare generală a standardelor existente în materia drepturilor fundamentale. Aceasta s-a axat pe mecanismele de control și pe căile de atac aflate la dispoziția persoanelor fizice care pretind că au loc încălcări ale dreptului lor la intimitate.

Cercetarea legală a FRA nu analizează tehnicile de supraveghere ca atare. Aceasta recapitulează modul în care cadrele juridice permit utilizarea acestor tehnici și explorează rolul crucial pe care îl joacă organele specializate în supravegherea activității serviciilor de informații. În plus, analizează cu atenție cât de mult măsurile de protecție respective protejează intimitatea și protecția datelor în cele 28 de state membre ale UE.

„Serviciile de informații" au un mandat extern și se concentrează pe amenințările externe, în timp ce „serviciile de securitate" au un mandat intern și se concentrează pe amenințările interne. Raportul FRA folosește termenul de „servicii de informații" ca termen general pentru ambele noțiuni.

Acest rezumat prezintă principalele constatări ale cercetărilor FRA, publicate integral în raportul intitulat *Supravegherea de către serviciile de informații: măsurile de protecție și căile de atac privind drepturile fundamentale în UE - Reprezentarea grafică a cadrelor juridice ale statelor membre* (a se vedea Informații suplimentare).

Colectarea datelor și acoperirea

Pentru acest studiu, FRA a examinat cadrele juridice privind supravegherea din cele 28 de state membre ale UE, analizând legile și standardele aferente ale drepturilor fundamentale pentru a prezenta o analiză comparativă a contextului juridic al supravegherii în UE.

Pe baza răspunsurilor furnizate de Franet, rețeaua de cercetare multidisciplinară a agenției, FRA a cules date și informații prin cercetare documentară în toate cele 28 de state membre ale UE. Au fost culese informații suplimentare prin schimburi cu partenerii principali, inclusiv cu o serie de funcționari naționali de legătură din statele membre, organe specializate și experți individuali. Constatările se inspiră și din rapoartele și publicațiile existente, menite să sprijine legiuitorii naționali în stabilirea cadrelor juridice pentru serviciile de informații și supravegherea lor democratică.

Un al doilea raport socio-legal cu opinii FRA, bazat pe cercetare empirică, va fi publicat într-o etapă ulterioară, extinzând și mai mult constatările prezentate aici.

Măsurile de protecție privind drepturile fundamentale și legislația UE

„Crudul adevăr este că folosirea eficientă a tehnologiei de supraveghere în masă înlătură cu desăvârșire dreptul la intimitatea comunicațiilor pe internet."
[Organizația Națiunilor Unite (ONU), Raportorul Special privind promovarea și protecția drepturilor omului și a libertăților fundamentale în cadrul luptei antiterorism (2014), *Al patrulea raport anual trimis Adunării Generale*, A/69/397, 23 septembrie 2014]

Statele membre ale UE sunt toate obligate să respecte standardele minime ale legislației internaționale privind drepturile omului, dezvoltate de Organizația Națiunilor Unite (ONU), care au o aplicabilitate universală, cum ar fi Hotărârea Consiliului Drepturilor Omului privind dreptul la intimitate în era digitală (Doc. A/HRC/28/L.27, 24 martie 2015).

Diferiți experți și organe convenționale ale ONU au condamnat practicile de supraveghere în masă ca urmare a dezvăluirilor lui Snowden. Standardele Consiliului Europei, inclusiv jurisprudența Curții Europene a Drepturilor Omului (CEDO), rezumă de asemenea standardele minime. În plus, mai este relevantă și jurisprudența UE, interpretată de Curtea de Justiție a Uniunii Europene (CJUE). În sfârșit, într-un domeniu în care se aplică direct numai reglementări internaționale limitate – altele decât legislația internațională existentă privind drepturile omului – sunt importante și măsurile de autoreglementare și legile neobligatorii.

Raportul se concentrează pe drepturile la intimitate și la protecția datelor, consfințite în articolele 7 și 8 ale cartei. Dreptul la protecția datelor este stipulat și în legislația europeană primară și secundară, garantând că, în domeniul de aplicare al acestora, prelucrarea datelor cu caracter personal se va face în mod legal și numai în măsura în care este necesar pentru a atinge scopul urmărit. Aceste drepturi se extind asupra tuturor persoanelor, indiferent că sunt cetățeni UE sau ai statelor terțe. Conform articolului 52 alineatul (1) din cartă, orice limitare a acestui drept trebuie să fie necesară și proporționată, să întrunească cu adevărat obiectivele de interes general recunoscute de Uniune, să fie prevăzută de lege și să respecte esența drepturilor respective.

În ciuda faptului că există orientări internaționale, nu există o înțelegere uniformă a „securității naționale" în întreaga UE. Nici legislația UE, nici jurisprudența CJUE nu definesc mai mult acest concept, deși CJUE a declarat că excepțiile de la drepturile fundamentale trebuie interpretate restrictiv și justificate.

Această descriere vagă a „securității naționale" are repercusiuni pentru aplicabilitatea legislației UE. Articolul 4 alineatul (2) din Tratatul privind Uniunea Europeană prevede că „securitatea națională rămâne responsabilitatea exclusivă a fiecărui stat membru". Acest lucru nu înseamnă că scutirea „securității naționale" face complet inaplicabilă legislația UE. Interpretarea „securității naționale" la nivelul statelor membre și modul în care sunt îndeplinite programele de supraveghere pot fi evaluate de instituțiile UE, în special de CJUE.

Tipuri de supraveghere: țintită și netțintită

Ancheta FRA examinează modul în care sunt organizate atât supravegherea țintită, cât și cea netințită în cadrele juridice ale statelor membre ale UE.

Comitetul Olandez de Verificare pentru Serviciile de Informații și de Securitate (CTIVD) definește supravegherea țintită și netințită după cum urmează:

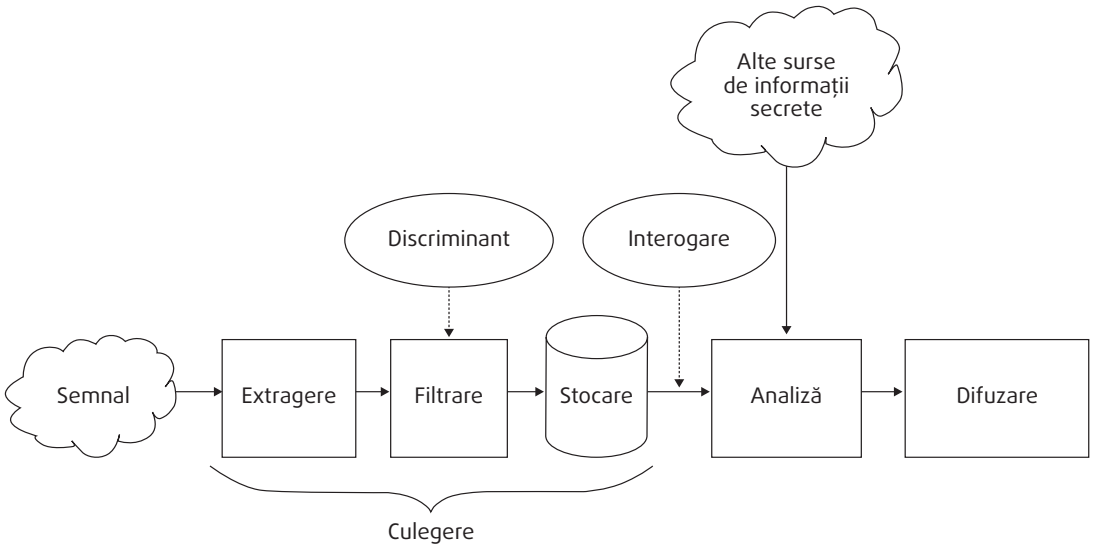
- interceptarea țintită se referă la „interceptarea în care persoana, organizația sau caracteristica tehnică către care este țintită culegerea de date poate fi specificată dinainte";
- interceptarea netințită se referă la „interceptarea în care persoana, organizația sau caracteristica tehnică către care este țintită culegerea de date nu poate fi specificată dinainte".

CTIVD, *Raport anual 2013–2014*, Haga, 31 martie 2014, pp. 45–46.

Amploarea datelor culese prin programele de supraveghere neacoperite – cum ar fi PRISM, Xkeyscore și Upstream – a atras reacții majore. „Supravegherea în masă" (adesea înțeleasă ca netințită) presupune culegerea unor cantități de date mult diferite de cele culese în cazul metodelor de supraveghere tradiționale, secrete (țintite), cum ar fi ascultarea convorbirilor telefonice. Aceasta din urmă se bazează pe suspectarea prealabilă a unei anumite persoane sau organizații. Acest tip de supraveghere este predominant în legislația statelor membre ale UE și recunoscut de aceasta. Majoritatea covârșitoare a cadrelor juridice ale statelor membre ale UE nu reglementează și nici măcar nu fac referire la „supravegherea în masă" ca atare. Numai câteva state membre ale UE au o legislație detaliată cu privire la informațiile din semnale (SIGINT), care este un termen generic folosit pentru a descrie interceptarea semnalelor din diferite surse de către serviciile de informații. Ancheta FRA folosește termenul de informații din semnale în întreaga sa analiză.

SIGINT vine de la informații secrete militare. Se referă la culegerea automată de informații prin interceptarea și culegerea de date digitale legate de activitatea de informații secrete. Figura evidențiază faptul că semnalele culese sunt filtrate cu ajutorul unor discriminanți sau selectori – o serie de parametri introduși în procesul de filtrare, fie *a priori*, fie dinamic, pentru a defini criteriile ce vor determina care date să fie stocate pentru a obține informațiile relevante (de exemplu: „toate adresele de e-mail folosite în comunicații cu Yemenul").

Figură: Modelul conceptual al informațiilor din semnale



Sursa: Statele Unite, Consiliul Național de Cercetare (2015), p. 28.

Consiliul Național de Cercetare al Statelor Unite din cadrul Academiilor Naționale a definit informațiile din semnale ca un termen cuprinzător pentru datele stocate pe un dispozitiv electronic. Comisia de la Veneția folosește SIGINT ca termen colectiv pentru mijloacele și metodele de interceptare și analiză a comunicațiilor radio (inclusiv satelit și telefoane mobile) și a celor prin cablu.

Analiza FRA a cadrelor juridice ce reglementează metodele de supraveghere a serviciilor de informații arată că legislația a cinci state membre ale UE (Franța, Germania, Țările de Jos, Suedia și Regatul Unit) detaliază condițiile ce permit folosirea unei supravegheri atât țintite, cât și nețintite, cum ar fi informațiile din semnale. Alte legi din statele membre precizează insuficient aceste condiții, îngreunând analiza legală a procedurilor exacte puse la punct pentru culegerea informațiilor din semnale. Chiar dacă legile din aceste țări nu se referă în mod specific la SIGINT, totuși aceasta se poate efectua. Cu toate acestea, având în vedere că practica este prescrisă numai în măsurile de reglementare nepublicate din aceste țări, o analiză a cadrelor juridice în vigoare nu va face lumină în această problemă.

Principalele constatări

Serviciile de informații și legile de supraveghere

Obiectivul și structura serviciilor de informații

Obiectivul principal al serviciilor de informații în societățile democratice este de a proteja securitatea națională și valorile fundamentale ale unei societăți deschise folosind instrumentele informațiilor secrete. Organizarea comunității de informații în statele membre individuale ale UE este strâns legată de evoluția istorică specifică fiecărei țări și nu respectă neapărat standardele drepturilor fundamentale. Ca urmare, serviciile de informații sunt constituite în moduri extrem de diverse în UE. În unele state membre, două servicii de informații execută munca, în timp ce în altele sunt responsabile cinci sau șase organe.

- Aproape toate statele membre ale UE au înființat cel puțin două servicii de informații diferite, unul pe probleme civile, celălalt pe probleme militare; cel din urmă nu este analizat în acest raport. Serviciile de informații civile sunt, în general, subordonate ministerelor de interne și uneori și prim-ministrului sau președintelui.

- În unele state membre, serviciile civile sunt subîmpărțite și mai mult, și anume într-un serviciu cu mandat intern și un serviciu cu mandat extern. Mai mult decât atât, unele state membre au încredințat măsuri de culegere de informații unităților specializate într-un anumit pericol, cum ar fi crima organizată, corupția sau lupta antiterorism.

Apărarea securității naționale

Ancheta FRA analizează noțiunea de „securitate națională" din perspectiva mandatului serviciilor de informații și a măsurilor de supraveghere pe care acestea le pot lua. Și de această dată, constatările scot în evidență o mare diversitate în rândul statelor membre ale UE.

- Obiectivul principal al serviciilor de informații este apărarea securității naționale, însă conceptul nu este armonizat în toate statele membre ale UE. Înțelesul termenului de securitate națională este rareori definit, uneori folosindu-se termeni similari. Alte state membre nu folosesc deloc termenul de „securitate națională", numind-o „securitate internă" și/sau „securitate externă" sau „securitatea statului".

- Obiectul diferitelor sarcini ale serviciilor de informații (adică mandatul lor) nu este identic în toate statele membre ale UE. Pe lângă domeniile mai tradiționale, mandatele unor servicii de informații includ și crima organizată și infracțiunile din sistemul cibernetic. Acești termeni nu sunt definiți în mod armonizat.

Reglementarea legală a supravegherii

Linia de demarcație dintre sarcinile organelor de aplicare a legii și cele ale serviciilor de informații este uneori neclară. Orice extindere a sarcinilor trebuie bine justificată ca necesară pentru apărarea statului, acesta fiind motivul de bază al înființării serviciilor de informații.

- Cadrele juridice ale celor mai multe state membre reglementează numai supravegherea țintită, fie a persoanelor fizice, fie a grupurilor/organizațiilor definite. Pe lângă abordarea supravegherii țintite, cinci state membre au adoptat legi detaliate referitoare la condițiile în care pot fi folosite informațiile din semnale.

- Dacă ne uităm la standardele în vigoare privind drepturile omului, din cadrele juridice naționale lipsesc definițiile care să indice categoriile de persoane și obiectul activităților ce pot fi supuse culegerii de informații.

- Serviciile de informații sunt reglementate prin lege în marea majoritate a statelor membre (26 din 28). Prevederile legale reglementează organizarea și funcționarea serviciilor de informații ale țărilor. Constituția unuia dintre statele membre interzice serviciului său de informații să efectueze supravegherea. Un alt stat membru este în curs de adoptare a unei legislații ce va reglementa practicile de supraveghere ale serviciilor sale de informații.

- Analiza FRA arată că temeiul legal ce încadrează mandatele și puterile serviciilor de informații naționale din statele membre ale UE variază de la o lege unică ce reglementează organizarea și mijloacele serviciilor naționale până la cadre legislative complexe ce constau din mai multe legi și ordonanțe ce reglementează aspecte specifice ale mandatului, organizării, competențelor sau mijloacelor acestora.

- Majoritatea statelor membre organizează munca serviciilor de informații prin două legi: o lege privind mandatul și organizarea serviciului și o altă lege privind mijloacele de acțiune și condițiile de utilizare a acestora.

- Majoritatea statelor membre ale UE (23 din 28) au separat serviciile de informații de autoritățile de aplicare a legii. Două state membre au renunțat recent la sistemele în care serviciile de informații aparțineau poliției sau unor autorități similare de aplicare a legii.

Supravegherea serviciilor de informații

Analiza FRA examinează mecanismele de responsabilizare referitoare la supravegherea de către serviciile de informații. Aceasta descrie în special modul în care statele membre ale UE au stabilit mecanismele de supraveghere. Supravegherea este un mod de a asigura responsabilizarea publică pentru deciziile și acțiunile serviciilor de informații. Conform experților, supravegherea are ca scop evitarea abuzului de putere, legitimizarea exercitării puterilor intruzive și atingerea unui rezultat mai bun după o evaluare a acțiunilor specifice. Consensul general, luat dintr-un raport al Comisiei de la Veneția și din alte studii academice, este că supravegherea ar trebui să fie o combinație de:

- control executiv;
- supraveghere parlamentară;
- corpuri de experți;
- control judiciar.

Controlul executiv și coordonarea dintre organele de supraveghere

Ramura executivă poate controla serviciile de informații în mai multe feluri: prin specificarea politicilor și priorităților lor strategice sau stabilirea unor orientări; prin numirea și/sau desemnarea conducerii superioare a serviciului; prin formularea bugetului asupra căruia va vota în final parlamentul; sau prin aprobarea cooperării cu alte servicii. De asemenea, executivul joacă un rol crucial în autorizarea măsurilor de supraveghere din unele state membre.

O supraveghere eficientă necesită o bună coordonare între diferitele organe de supraveghere pentru a asigura acoperirea fiecărui aspect al muncii serviciilor de informații. În cazul în care organele de supraveghere nu înțeleg în mod clar și cuprinzător munca întregii comunități naționale de informații, vor apărea goluri în supraveghere, iar eficiența sistemului de supraveghere ca întreg va avea de suferit.

- Diversitatea din statele membre ale UE în materie de politică și sisteme juridice s-a tradus într-o mare varietate de organe ce supraveghează serviciile de informații. Statele membre ale UE au sisteme de supraveghere mult diferite. Deși bunele practici pot fi extrase din sistemele aflate în funcțiune, sectoarele individuale ar avea de câștigat de pe urma unei reforme juridice care ar spori puterea organelor de supraveghere.

- O mare gamă de puteri este acordată diferitelor organe de supraveghere, iar măsura în care acestea le pot exercita variază și ea.

- Șapte state membre au sisteme de supraveghere ce combină organe executive, parlamentare, judiciare (prin aprobare *ex ante*) și de experți. Totuși, printre acestea nu se numără niciuna dintre țările cu cadre juridice ce permit culegerea de informații din semnale.

- O supraveghere eficientă nu necesită neapărat toate patru tipurile de mecanisme de supraveghere. Această supraveghere poate fi realizată câtă vreme organele existente se completează unul pe altul și, ca întreg, constituie un sistem puternic de evaluare dacă mandatul serviciilor de informații este dus la îndeplinire cum se cuvine. Acest lucru va avea loc dacă puterile de supraveghere acoperă toate sectoarele de activitate ale unui serviciu de informații. Atunci când mandatul în sine este însă neclar sau insuficient dezvoltat, organele de supraveghere nu vor putea să exercite nicio influență.

- Accesul organelor de supraveghere la informații și la documente este esențial. Deși informațiile culese de serviciile de informații sunt sensibile, iar măsurile de protecție trebuie să garanteze faptul că vor fi prelucrate în conformitate, organele de supraveghere nu-și pot îndeplini sarcinile fără a avea mai întâi acces la toate informațiile relevante. Cu toate acestea, opusul pare să fie regula.

Supravegherea parlamentară

Supravegherea parlamentară este importantă, având în vedere responsabilitatea parlamentului de a trage la răspundere guvernul. Parlamentul, ca legiuitor, răspunde de adoptarea unei legislații clare, accesibile, care să instituie serviciile de informații și să le precizeze organizarea, puterile speciale și limitările. De asemenea, parlamentul are sarcina de a aproba bugetul serviciilor de informații, iar în anumite state membre cercetează dacă operațiunile acestora respectă cadrul legal.

- Constatările FRA arată că 24 de state membre ale UE folosesc supravegherea parlamentară; în 21 dintre acestea, serviciile de informații sunt supravegheate de comisii parlamentare speciale. Unele state membre au constituit o comisie parlamentară care să se ocupe de diferitele servicii de securitate și de informații, în timp ce altele au înființat comisii diferite care să se ocupe de fiecare serviciu în parte.

- În niciun stat membru comisia parlamentară nu deține un drept de acces nelimitat la informațiile serviciilor.

- Diferitele comisii parlamentare din statele membre au mandate diferite: majoritatea au competențe de supraveghere tradiționale în legătură cu legislația, bugetul și primirea informațiilor legate de funcția serviciilor, în timp ce numai câteva se pot ocupa de reclamații, pot adopta decizii obligatorii pentru serviciile de informații sau pot ajuta la aprobarea măsurilor de supraveghere.

- În ceea ce privește puterea comisiilor parlamentare de a demara investigații, legile celor mai multe țări permit acestor comisii să solicite informații de la serviciile de informații sau de la executiv, dar nu să le ceară imperativ.

Supravegherea de către experți

Supravegherea de către experți este deosebit de valoroasă, deoarece le permite persoanelor fizice familiarizate cu subiectul să își facă timp să se dedice problemei, fiind independente de loialitățile politice în examinarea acțiunilor serviciilor de informații. Conform Comisarului pentru Drepturile Omului al Consiliului Europei, acești experți sunt deseori cei mai în măsură să realizeze supravegherea zilnică a activității serviciilor de securitate și de informații.

- Deși supravegherea parlamentară este esențială, ea trebuie completată de organe de supraveghere, în special de corpuri de experți puternice care să poată supraveghea activitățile operaționale, inclusiv culegerea, schimbul și utilizarea datelor cu caracter personal, precum și protecția dreptului la viață privată.

- În UE, 15 state membre au constituit unul sau mai multe corpuri de experți dedicate exclusiv supravegherii serviciilor de informații. Printre competențele acestora se numără autorizarea măsurilor de supraveghere, investigarea reclamațiilor, solicitarea de documente și informații din partea serviciilor de informații și acordarea de consiliere pentru executiv și/sau parlament. Pentru a-și maximiza potențialul, aceștia trebuie să beneficieze de independența, resursele și puterile adecvate.

- În unele state membre, autorizarea măsurilor de supraveghere nu implică nicio instituție independentă de serviciile de informații și de executiv.

- În statele membre care au un organ independent care să autorizeze măsurile de supraveghere, supravegherea țintită tinde să necesite aprobarea judiciară, în timp ce aprobarea prin corpuri de experți este cealaltă soluție preferată. Nu există nicio abordare comună în supravegherea culegerii de informații din semnale.

- Deși înțelegerea aspectelor juridice ale supravegherii este indispensabilă, corpurile de experți trebuie și să fie competente din punct de vedere tehnic. Unele state membre asigură acest lucru prin includerea unor experți dintr-o serie de domenii, inclusiv tehnologia informației și comunicațiilor (TIC). Altele se bazează pe o combinație de judecători și parlamentari actuali sau foști.

În statele membre ale UE, autoritățile pentru protecția datelor (*data protection authorities* – DPA) – organe specializate chemate să apere intimitatea și protecția datelor – au primit un rol fundamental în protecția datelor cu caracter personal. Acest rol este consfințit în legislația europeană primară și secundară. Însă corpurile de experți specializate în supravegherea serviciilor de informații au fără îndoială o expertiză recunoscută în intimitate și protecția datelor în domeniul informațiilor secrete.

- Constatările FRA arată că, comparativ cu alte activități de prelucrare a datelor și cu alți controlori de date din sectorul public și privat, DPA din șapte state membre au aceeași putere asupra serviciilor de informații ca și controlorii asupra tuturor celorlalte date. În 12 state membre, DPA nu au nicio competență asupra serviciilor de informații, iar în nouă state membre puterile lor sunt limitate.

- În statele membre în care DPA și alte corpuri de experți în supraveghere își împart competența, o lipsă de cooperare între aceștia ar putea lăsa goluri rezultate din responsabilitățile fragmentate. În statele membre în care DPA nu au competență asupra serviciilor de informații, organul de supraveghere are obligația de a se asigura că măsurile de protecție a intimității și a datelor sunt corect aplicate.

- Cercetările din trecut ale FRA în domeniul accesului la căile de atac în domeniul protecției datelor identifică nevoia de a îmbunătăți capacitatea DPA; acest lucru este important, având în vedere rolul pe care DPA l-ar putea juca în supravegherea serviciilor de informații.

Căile de atac

În conformitate cu standardele internaționale în vigoare, oricine suspectează că este victima unei încălcări a intimității sau a protecției datelor trebuie să poată avea posibilitatea de a încerca să remedieze situația. Dreptul la o cale de atac eficientă – care le permite persoanelor fizice să solicite despăgubiri pentru o încălcare a drepturilor lor – este o componentă esențială a accesului la justiție. O cale de atac trebuie să fie „efectivă" în fapt și în drept.

Așa cum arată rapoartele anterioare ale FRA privind accesul la căi de atac privind protecția datelor și accesul la justiție, victimele unor încălcări ale intimității și ale protecției datelor au la dispoziție o serie de căi de remediere. Organele nejudiciare joacă un rol de remediere important în domeniul supravegherii, având în vedere dificultățile practice în accesarea instanțelor generale. Organele nejudiciare din cele 28 de state membre ale UE cuprind corpuri de experți (inclusiv DPA), organe executive și parlamentare, precum și instituții mediatoare. În unele state membre, numărul organelor nejudiciare cu roluri de remediere în domeniul supravegherii este relativ încurajator, însă ar trebui privit din perspectiva următoarelor constatări.

Nici complexitatea cadrului de remediere, nici cantitatea de date culese de serviciile de informații care practică SIGINT nu facilitează implementarea unor căi de atac eficiente. Fragmentarea și compartimentarea diferitelor căi de remediere au făcut dificilă accesarea căilor de atac. De fapt, datele culese arată că numai un număr limitat de cazuri ce pun la încercare practicile de supraveghere au fost adjudecate la nivel național de la data dezvăluirilor lui Snowden încoace.

Obligația de informare și dreptul de acces

Dreptul de a fi notificat și de a avea acces la informații este crucial pentru alertarea persoanelor fizice față de măsurile de supraveghere și pentru demararea unei acțiuni de remediere. Curtea Europeană a Drepturilor Omului (CEDO) a acceptat însă faptul că aceste drepturi pot fi limitate în mod justificabil (a se vedea CEDO, *Klass și alții v. Germania*, nr. 5029/71, 6 septembrie 1978). Constatările FRA arată că secretul din jurul activității serviciilor de informații limitează într-adevăr aceste drepturi. Un alt factor este numărul mare de date culese prin SIGINT comparativ cu formele mai tradiționale de supraveghere.

- În opt state membre, obligația de informare și dreptul de acces nu sunt prevăzute deloc de lege; se aplică regulile privind documentele clasificate sau secretele de stat. În celelalte 20 de state membre, legislația prevede obligația de informare și dreptul de acces, în unele cazuri în intervale de timp specifice, deși cu restricții. Aceste restricții cuprind diferite motive, cum ar fi securitatea națională, interesele naționale sau scopul măsurii de supraveghere în sine.

- Numai două state membre au prevederi specifice privind obligația de informare în contextul informațiilor din semnale: într-unul din aceste state, persoanele fizice nu sunt informate dacă selectorii folosiți nu sunt direct atribuibili persoanei fizice; în celălalt stat, persoana fizică nu este informată dacă datele personale obținute sunt șterse imediat după culegere și nu mai sunt prelucrate.

- Organele de supraveghere din 10 state membre, inclusiv șase DPA naționale, revizuiesc restricțiile privind dreptul de a fi informat și dreptul de a accesa informațiile verificând dacă pericolul național pentru securitate invocat este rezonabil și/sau exercitând indirect dreptul de acces al persoanei fizice. În al doilea caz, organele evaluează dacă accesul la date poate fi acordat sau dacă refuzul de a face acest lucru este legitim și analizează legalitatea prelucrării datelor. Într-un singur stat membru este necesar un mandat judiciar – care certifică faptul că notificarea ar pune în pericol investigația sau că există alte argumente împotriva acesteia.

- Alte două state membre nu acordă un drept de acces la informații ca atare. Legea prevede însă un drept care produce același rezultat: o persoană fizică îi poate cere organului de supraveghere să verifice dacă datele sale sunt supuse unei supravegheri nelegale.

- În unele state membre, organul de supraveghere implicat în exercitarea indirectă a dreptului unei persoane fizice de a solicita accesul la date nici nu confirmă, nici nu neagă prelucrarea datelor. Răspunsurile sunt de obicei limitate la a afirma că plângerea a fost prelucrată și/sau verificată.

Căile de atac judiciare

Fiecare stat membru le oferă persoanelor fizice ocazia de a face plângere în legătură cu încălcările de intimitate prin intermediul instanțelor, indiferent dacă acestea au avut loc ca urmare a unor informații țintite sau din semnale. Instanțele oferă o cale pentru persoanele fizice de a se plânge cu privire la încălcarea intimității lor, inclusiv de a contesta hotărârile organului de supraveghere referitoare la afirmațiile lor de încălcare a intimității. De asemenea, ele le oferă persoanelor fizice o ocazie de a accesa căile de atac – inclusiv în domeniul supravegherii.

- Cercetările din trecut ale FRA au identificat însă lipsa de specializare a judecătorilor în protecția datelor ca pe un obstacol serios în calea remedierii eficiente a încălcărilor de protecție a datelor. Această constatare este relevantă pentru supraveghere, unde, pe lângă secretul necesar legat de informațiile secrete, expertiza relevantă în TIC sau în informații secrete, de exemplu, este esențială.

- Numai două state membre au diminuat lipsa de specializare cu privire la căile de atac, implicând judecători/instanțe care au la dispoziția lor atât cunoștințele necesare pentru a hotărî în probleme (adesea) tehnice, cât și permisiunea de a accesa materiale secrete.

Căile de atac nejudiciare

Opțiunile nejudiciare sunt de obicei mai accesibile persoanelor fizice decât mecanismele judiciare, deoarece regulile de procedură sunt mai puțin stricte, a face plângere este un lucru mai puțin costisitor, iar procedurile se desfășoară mai rapid. Dovezile din trecut ale FRA confirmă acest lucru, în special în contextul protecției datelor, deoarece există tendința de a depune mai multe plângeri la DPA naționale și mai puțini reclamanți urmează calea procedurii judiciare. Totuși, numărul de organe nejudiciare – altele decât DPA – care se pare că activează în domeniul protecției datelor este mic și multe organe nejudiciare au numai o putere limitată de a oferi măsuri corective.

- Organele de supraveghere (inclusiv DPA) însărcinate cu soluționarea plângerilor sunt instituții independente în marea majoritate a statelor membre.

- Când un organ de supraveghere executiv deține puteri reparatorii, apare problema independenței atunci când are și puterea de a autoriza supravegherea. Organele de supraveghere parlamentare și corpurile de experți au structuri administrative mai autonome, însă autonomia nu garantează o cale de atac eficientă decât dacă este susținută de suficiente cunoștințe. Modul în care sunt numiți membrii organelor de supraveghere și locul lor în ierarhia administrativă sunt alte aspecte importante de luat în considerare la evaluarea independenței unui organ.

- DPA din 13 state membre ale UE au competența de a analiza plângerile persoanelor fizice și de a adopta hotărâri obligatorii. Însă, în trei dintre ele, competența de a accesa dosarele și spațiile este limitată. În cinci state membre se aplică cerințe suplimentare, necesitând prezența șefului sau a unui membru al DPA în timpul inspecțiilor organizate în spațiile serviciului de informații.

- Cinci din cele șapte state membre care le încredințează organelor de supraveghere formate din experți (altele decât DPA) competențe reparatorii specifice fac acest lucru permițându-le acestor organe să adopte hotărâri obligatorii. În două state membre un organ de supraveghere executiv are și puteri reparatorii. Comisiile parlamentare din patru state membre au dreptul de a fi sesizate cu plângeri ale persoanelor fizice, însă numai una le poate soluționa cu hotărâri obligatorii.

- Instituțiile mediatoare, care există în toate cele 28 de state membre ale UE, se ocupă în principal de lacunele administrative, mai degrabă decât de meritele efective ale supravegherii. Un singur stat membru oferă instituției mediatoare puteri reparatorii prin legea informațiilor adoptată în materie. În plus, puterile instituțiilor mediatoare pot fi destul de limitate, iar procedurile se încheie de obicei cu recomandări neobligatorii menite să îndrepte lucrurile și să ghideze acțiunile viitoare, și nu cu o sentință obligatorie, executorie. Acest lucru are în mod evident un impact asupra eficienței reparațiilor pe care sunt capabile să le ofere.

- Printre alte elemente ce facilitează accesul unei persoane fizice la căile de atac se numără regulile mai relaxate privind sarcina probei și acțiunile colective, precum și protecția efectivă a avertizorilor. Adunarea Parlamentară a Consiliului Europei consideră denunțarea ca fiind cel mai eficient instrument pentru implementarea limitelor puse pe supraveghere.

Concluzii

Abordând un domeniu de competență a UE limitată, raportul evidențiază diversitatea în rândul statelor membre cu privire la modul în care serviciile de informații sunt organizate și își îndeplinesc sarcinile principale.

Măsurile de supraveghere afectează foarte mult drepturile persoanelor fizice. Având în vedere natura lor secretă, persoanele fizice sunt obligate să se bazeze pe o anumită încredere în autoritățile publice, care în schimb sunt obligate să apere drepturile fundamentale ale persoanelor fizice. Pentru a atinge nivelul de încredere pe care o societate ar trebui să îl aibă față de serviciul său de informații este nevoie de responsabilitate. O legislație clară și accesibilă, niște mecanisme de supraveghere puternice, niște mecanisme de control adecvate și căi de atac eficiente sunt numai câteva dintre elementele esențiale pentru a atinge acest grad de responsabilitate, care rămâne incontestabil dificil din cauza secretului cu care lucrează serviciile de informații. Introducerea și menținerea unei legislații clare și accesibile și a unor puternice mecanisme de supraveghere la nivel de stat membru nu constituie decât primul pas către un sistem transparent și fundamental de respectare a drepturilor – dacă există dificultăți în realizarea acestui lucru, înseamnă că mai sunt obstacole de depășit.

Reacțiile la dezvăluirile lui Snowden au evidențiat nevoia de a adapta și de a consolida cadrele juridice relevante în UE și în toate statele membre ale acesteia. Cercetarea FRA arată că au fost deja efectuate o serie de reforme juridice. Evaluările periodice ale funcționării și legitimității cadrelor juridice ce guvernează activitatea serviciilor de informații trebuie să devină parte integrantă din sistemele de supraveghere. O altă întrebare-cheie este cum să reformăm în continuare cadrele juridice pentru a aborda lipsa de supraveghere adecvată. În plus, reformele din statele membre ale UE trebuie să ia în considerare evoluțiile tehnologice recente pentru a se asigura că mecanismele de supraveghere beneficiază de instrumentele necesare și de cunoștințele experților. Realizarea acestor planuri este fără îndoială complexă, însă vitală pentru realizarea dificilei sarcini de a proteja securitatea, apărând în același timp drepturile fundamentale.

Protejarea publicului împotriva pericolelor la adresa securității și apărarea drepturilor fundamentale necesită un echilibru delicat. Atacurile teroriste brutale și inovațiile tehnologice care fac posibilă monitorizarea datelor de comunicații pe scară largă au complicat și mai mult problema, dând naștere unor preocupări legate de încălcări ale drepturilor la intimitate și la protecția datelor în numele protecției securității naționale. Dezvăluirile lui Snowden, ce au dat în vileag eforturi de supraveghere considerabile și nediscriminate în întreaga lume, au arătat în mod clar că sunt necesare măsuri de protecție sporite pentru aceste drepturi.

Prezentul raport, redactat ca urmare a cererii Parlamentului European de a efectua o cercetare amănunțită asupra protecției drepturilor fundamentale în contextul supravegherii, cartografiază și analizează cadrele juridice privind supravegherea implementate în statele membre ale UE. Concentrându-se pe așa-zisa „supraveghere în masă", acesta detaliază și mecanismele de supraveghere introduse în întreaga UE, sintetizează activitatea entităților însărcinate cu verificarea eforturilor de supraveghere și prezintă căile de atac aflate la dispoziția persoanelor fizice care doresc să conteste această activitate de culegere a informațiilor. Prin demonstrarea considerentelor complexe ce intră în discuție, prezentul raport subliniază cât de dificilă poate fi abordarea a ceea ce este adeseori văzut ca o concurență a priorităților și contribuie la dezbaterea continuă asupra modului în care ar trebui reconciliate cel mai bine.

Informații suplimentare:

Pentru raportul FRA complet, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Supravegherea de către serviciile de informații: măsurile de protecție și căile de atac privind drepturile fundamentale în UE – Reprezentarea grafică a cadrelor juridice ale statelor membre), a se vedea: http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

A se vedea și alte publicații ale FRA din acest domeniu:

- FRA, CEDO, Consiliul Europei (2014), *Manual de legislație europeană privind protecția datelor*, Luxemburg, Oficiul pentru Publicații, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (disponibil în 23 de limbi oficiale ale UE)
- FRA (2014), *Access to data protection remedies in EU Member States* (Accesul la căile de atac în domeniul protecției datelor cu caracter personal în statele membre ale UE), Luxemburg, Oficiul pentru Publicații, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states, precum și rezumatul raportului http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary (disponibil în 21 de limbi oficiale ale UE)

O prezentare generală a activităților FRA cu privire la protecția datelor este disponibilă la adresa: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Oficiul pentru Publicații

FRA – AGENȚIA PENTRU DREPTURI FUNDAMENTALE A UNIUNII EUROPENE

Schwarzenbergplatz 11 – 1040 Viena – Austria
Telefon: +43 158030-0 – Fax: +43 158030-699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Print: ISBN 978-92-9491-024-0, doi:10.2811/87845
PDF: ISBN 978-92-9491-023-3, doi:10.2811/192567

TK-04-15-738-RO-C (print); TK-04-15-738-RO-N (PDF)