Strasbourg, 11 decembrie 2024 **CDL-AD(2024)043**
(*Traducere neoficială*)

Comisia Europeană pentru Democrație prin Drept
(Comisia de la Veneția)

RAPORT

CU PRIVIRE LA

O REGLEMENTARE A PROGRAMELOR SPION CONFORMĂ CU STATUL DE DREPT ȘI DREPTURILE OMULUI

adoptat de Comisia de la Veneția
la cea de-a 141-a Sesiune plenară
(Veneția, 6-7 decembrie 2024)

pe baza comentariilor formulate de:

dl Iain CAMERON (membru, Suedia)
dl David A. KAYE (membru, Statele Unite ale Americii)
dl Tuomas OJANEN (membru, Finlanda)
dl Timothy OTTY (membru, Marea Britanie)
dna Tamar KALDANI (expert, Georgia)

Cuprins:

I. Introducere

1. Printr-o scrisoare din 6 decembrie 2023, Președintele de atunci al Adunării Parlamentare a Consiliului Europei (APCE), dl Tiny Kox, i-a solicitat Comisiei de la Veneția, în conformitate cu Rezoluția 2513 (2023) a APCE privind „Programul spion Pegasus și programele de tip spion similare și supravegherea secretă a statului”,[1] efectuarea un studiu referitor la cadrul legislativ și practica tuturor statelor membre ale Consiliului Europei privind supravegherea țintită (în mod prioritar Polonia, Ungaria, Grecia, Spania și Azerbaidjan; ulterior Germania, Belgia, Luxemburg, Țările de Jos și toate celelalte state membre).

2. Prin Rezoluția 2513(2023), APCE le-a solicitat unor state membre să o informeze pe ea, precum și pe Comisia de la Veneția, cu privire la utilizarea programului spion Pegasus și a programelor de tip spion similare[2] sau să elucideze cadrul juridic referitor la utilizarea lor și orice mecanisme de control aplicabile.[3] În special, APCE i-a solicitat Comisiei de la Veneția să evalueze cadrul legislativ și practica tuturor statelor membre privind supravegherea țintită (în mod prioritar cele vizate de Rezoluție), pentru a evalua dacă astfel de cadre conțin garanții adecvate și eficiente împotriva oricărui posibil abuz de programe spion, având în vedere Convenția și alte standarde ale Consiliului Europei.[4]

3. Dnii Iain Cameron, David A. Kaye, Tuomas Ojanen şi Timothy Otty au acţionat în calitate de raportori pentru acest raport. Dna Tamar Kaldani, fost Prim-Vicepreședinte și membru ales al Comitetului Consultativ al Convenției 108 a Consiliului Europei, a fost invitată să se alăture grupului de lucru în calitate de expert.

4. Ca răspuns la cerere, Comisia de la Veneția a efectuat un studiu comparativ pentru a evalua regulile existente privind supravegherea țintită și, în special, privind utilizarea programelor spion în statele sale membre. Comisia de la Veneţia a analizat prevederile legale ale statelor care au trimis informaţii oficiale către APCE[5] şi a celor asupra cărora membrii Comisiei/experţii de la Veneţia au prezentat informaţii, răspunzând la un chestionar pregătit de raportori (CDLPI(2024)014).[6] Informații suplimentare au fost colectate prin cercetări documentare.[7] Materialul colectat este disponibil în funcție de țară și întrebare.

---

[1] APCE, Rezoluția 2513(2023), Pegasus și programele spion similare și supravegherea secretă efecuată de către stat, 11 octombrie 2023. După cum se explică în rezoluție și detaliat mai jos, Pegasus este un program spion dezvoltat de o companie israeliană, NSO și este acum probabil cel mai cunoscut dintre diferitele programe spion utilizate de state în ultimii ani.
[2] Polonia, Ungaria, Grecia, Spania și Azerbaidjan, § 11 din Rezoluție.
[3] Germania, Belgia, Luxemburg și Țările de Jos, § 13 din rezoluție.
[4] § 15 din Rezoluție.
[5] APCE a împărtășit Comisiei de la Veneția răspunsurile primite, și anume din Azerbaidjan, Germania, Grecia, Luxemburg, Țările de Jos, Polonia și Spania. Belgia și Ungaria nu au trimis răspunsuri.
[6] Au fost primite răspunsuri la acest chestionar și la o solicitare mai generală de informații, trimisă în februarie 2024, în care raportorii au solicitat informații despre cadrul juridic care reglementează utilizarea Pegasus și a altor programe spion echivalente, din partea Austriei, Belgiei, Bulgariei, Bosniei și Herțegovinei, Canadei, Croației, Ciprului, Danemarcei, Estoniei, Finlandei, Franței, Germaniei, Greciei, Islandei, Irlandei, Italiei, Kosovo, Kârgâzstan, Liechtenstein, Lituania, Malta, Republica Moldova, Monaco, Maroc, Țările de Jos, Macedonia de Nord, Norvegia, Polonia, Portugalia, România, San Marino, Serbia, Republica Slovacă, Coreea de Sud, Spania, Suedia, Elveția, Turcia, Ucraina, Regatul Unit, Statele Unite ale Americii.
[7] A se vedea, în special, Parlamentul European, Utilizarea Pegasus și a programelor spion de supraveghere echivalente - Cadrul juridic existent în statele membre ale UE pentru achiziționarea și utilizarea Pegasus și a programelor spion de supraveghere echivalente („Studiul PEGA”), 5 decembrie 2022 și raportul Agenției pentru Drepturi Fundamentale, Supravegherea de către serviciile de informații: garanții și căi de atac ale drepturilor fundamentale în UE - actualizare din 2023 („Raportul FRA”), 24 mai 2023. Raportul FRA oferă o actualizare parțială a rapoartelor FRA din 2015 și 2017.

5. Raportul a fost elaborat pe baza comentariilor raportorilor și a rezultatelor cercetării comparative. Acesta a fost adoptat de Comisia de la Veneția la cea de-a 141-a Sesiune plenară (Veneția, 6-7 decembrie 2024).

II. Contextul și domeniul de aplicare al raportului

6. Există mai mulți termeni care se referă la tipul de supraveghere vizată în cauză: „program spion", „program de supraveghere intruzivă" sau termenul mai neutru „exploatarea rețelelor informatice". În acest raport, Comisia de la Veneţia va folosi termenul „program spion", care este folosit şi în cererea APCE.

7. Termenul „program spion" este un termen generic care cuprinde programe de supraveghere intruzivă care pot fi utilizate pentru a interfera cu dispozitive electronice, în special smartphone-uri sau calculatoare, fără știrea utilizatorului, și care-i permite operatorului să pătrundă în dispozitiv și, în funcție de instrumentul specific, să urmărească geo-localizarea în timp real, să citească toate datele stocate și toate comunicațiile efectuate (prin eludarea oricăror mecanisme de protecție, cum ar fi criptarea) și să preia controlul asupra oricăror materiale și programe disponibile pe dispozitiv, inclusiv microfoane sau camere.[8] Spre deosebire de interceptările telefonice clasice, programele spion pot oferi eventual acces complet și retroactiv la fișierele și mesajele create în trecut, parole și meta-date despre comunicațiile anterioare. Articolul 2 para. 20 din Regulamentul UE 2024/1083 (legislația europeană privind libertatea mass-media) definește „programul de supraveghere intruzivă"[9] drept "*orice produs cu elemente digitale special concepute pentru a exploata vulnerabilitățile din alte produse cu elemente digitale care permit supravegherea secretă a persoanelor fizice sau juridice prin controlul, extragerea, colectarea sau analizarea datelor care provin de la astfel de produse sau de la persoanele fizice sau juridice care utilizează astfel de produse, inclusiv într-un mod nediscriminatoriu*".[10]

8. Programele spion pot infecta dispozitivele vizate printr-o varietate de mecanisme: pot fi implantate prin acces fizic la un dispozitiv, dar și prin implantarea de la distanță a unui „trojan", a unui virus sau a unui program. Aceasta poate implica trimiterea unui mesaj (cum ar fi SMS, e-mail sau aplicații de mesagerie online) care să includă un link către o pagină web care, dacă este vizitat, va infecta dispozitivul. Unele instrumente folosesc așa-numitul atac „zero-click", în care simpla recepționare a unui mesaj provoacă infecția programului spion, fără a fi necesară vreo interacțiune a utilizatorului. Detectarea infecțiilor prin programe spion necesită competențe tehnice de nivel înalt, iar prezența lor pe un dispozitiv poate fi dificil de probat.[11] Cele mai intruzive programe spion, cum ar fi Pegasus, pot transforma in secret un telefon mobil sau un calculator personal într-un dispozitiv de supraveghere de 24 de ore din 24, permițând accesului complet al unui operator la toți senzorii și la toate informațiile de pe dispozitivul personal.

[8] Termenul „program spion" ca atare nu este folosit în legislația examinată de Comisia de la Veneția. A se vedea, de asemenea, para. 40 de mai jos.
[9] Considerentul 25 din Legea europeană privind libertatea mass-mediei include „programul spion" în sensul de „program de supraveghere intruziv".
[10] Regulamentul (UE) 2024/1083 al Parlamentului European și al Consiliului din 11 aprilie 2024 de instituire a unui cadru comun pentru serviciile mass-media pe piața internă și de modificare a Directivei 2010/13/UE (Actul european privind libertatea mass-mediei). Legea privind libertatea mass-mediei a intrat în vigoare la 7 mai 2024 și se va aplica integral începând cu 8 august 2025.
[11] Ibidem, p. 7 ff.

9. Utilizarea abuzivă a programelor spion comerciale a condus la încălcări foarte grave ale drepturilor omului. O coaliție internațională de jurnaliști de investigație a raportat că peste 50 000 de persoane, inclusiv apărători ai drepturilor omului, oponenți politici, avocați, diplomați, șefi de state și aproape 200 de jurnaliști din 24 de țări au fost identificați ca potențiale ținte ale programelor spion de stat.[12] Raportul APCE a constatat că există tot mai multe probe că Pegasus și programe spion similare au fost utilizate ilegal sau în scopuri nelegitime de către mai multe state membre, inclusiv împotriva jurnaliștilor, oponenților politici, apărători ai drepturilor omului și avocați.[13] APCE a relevat, de asemenea, probe că statele membre ale Consiliului Europei au exportat sisteme de supraveghere intruzivă cu caracteristici similare cu Pegasus către state terțe cu regimuri autoritare și cu un risc ridicat de încălcare a drepturilor omului.

10. Mai multe programe diferite de tip spion au fost dezvoltate, utilizate și exportate de către sau pentru state din întreaga lume. Extinderea considerabilă a comunicațiilor digitale a determinat statele să găsească instrumente care să permită supravegherea în contextul aplicării legii și al obținerii informațiilor. Cu referire la rețelele naționale de telecomunicații, statele au impus furnizorilor de telecomunicații obligația de a permite serviciilor de poliție și de informații accesul la comunicații într-o formă accesibilă, ocolind criptarea, care a devenit normă pentru furnizorii de telecomunicații și producătorii de dispozitive. În unele jurisdicții, în special atunci când suspectul cunoaște faptul că el/ea este investigat, este posibil ca o instanță să dispună producătorului sau furnizorului să „deschidă" dispozitivul. Cu toate acestea, serviciile de poliție și de informații au susținut că, atunci când o instanță nu este în măsură să pună în aplicare o astfel de ordonanță împotriva producătorului sau a furnizorului, și, prin urmare, nu este disponibil un acces dispus de instanță, este necesar să se obțină accesul într-un fel sau altul chiar la dispozitivele de comunicații (laptopuri, telefoane mobile etc.).

11. Statele afirmă în continuare necesitatea utilizării programelor spion pentru a apăra securitatea națională și publică împotriva amenințărilor, inclusiv a criminalității, și împotriva activităților care vizează destabilizarea structurilor lor fundamentale constituționale, politice, economice sau sociale. Evoluțiile tehnologice limitează capacitatea autorităților de aplicare a legii de a accesa date prin metode stabilite anterior. Ca urmare, unele state susțin că supravegherea intruzivă a dispozitivului suspectului este necesară pentru a-și finaliza investigațiile, în special pentru a avea acces la date altfel protejate prin criptare.[14]

---

[12] Istorii interzise, Proiectul Pegasus: o colaborare mondială pentru combaterea unei infracțiuni globale, 18 iulie 2021.

[13] Adunarea Parlamentară a Consiliului Europei, Raportul nr. 15825, programul spion Pegasus și alte tipuri de programe similare și supravegherea secretă efectuată de către stat („Raportul APCE"), 20 septembrie 2023, Expunere de motive §§ 6-63.

[14] După cum a constatat Comitetul permanent belgian pentru supravegherea serviciilor de informații și securitate: „Fără a nega importanța continuă a metodelor și tehnicilor de informații mai tradiționale, cum ar fi colectarea și analiza de informații umane „HUMINT" (Human Intelligence), este incontestabil că utilizarea instrumentelor tehnologice de informații și de securitate, cum ar fi tehnologiile de infecție la distanță, este de natură să consolideze în mod semnificativ poziția informațională a serviciilor. […] Trebuie spus că scăderea eficacității măsurilor mai tradiționale de interceptare a comunicațiilor este demonstrată de complexitatea crescândă a colectării și procesării informațiilor. Această situație împiedică din ce în ce mai mult, dacă nu împiedică, ciclul de informații și obiectivele sale de a anticipa riscurile de securitate și de a oferi autorităților consiliere adecvată cu privire la modul de a face față amenințărilor sau chiar de a le împiedica în mod direct"; a se vedea Comitetul permanent pentru supravegherea serviciilor de informații și securitate, monitorizarea investigației în urma dezvăluirilor privind utilizarea software-ului PEGASUS, 17 octombrie 2022. A se vedea, de asemenea, Camera Comunelor, Canada, Instrumente de investigare a dispozitivelor utilizate de Poliția Regală Canadiană și aspecte conexe – Raportul Comitetului permanent pentru accesul la informații, protecția informațiilor personale și etică, noiembrie 2022, secțiunea privind avantajele instrumentelor tehnologice de investigație, pp. 8-9.

12. Cu toate acestea, după cum reiese din descrierea preliminară a capacităților programelor spion prezentate mai sus, riscul de supraveghere intruzivă nejustificată sau disproporționată prin utilizarea unui astfel de instrument este important. Dacă nu sunt reglementate, programele spion constituie o armă puternică de supraveghere care poate fi folosită pentru a restrânge drepturile omului, a cenzura și incrimina criticile și disidența, pentru a hărțui (sau chiar suprima) jurnaliștii, apărărorii drepturilor omului, oponenții politici şi pentru a reprima organizaţiile societăţii civile. Rapoarte de expertiză substanțială stabilite de către organizații ale societății civile – în special de Citizen Lab[15], Amnesty Tech[16], și AccessNow[17]- au permis identificarea unor probe semnificative ale supravegherii abuzive folosind programe de tip spion.

13. Utilizarea programelor de tip spion de către forțele de ordine sau de serviciile de informaţii constituie un exemplu de „supraveghere țintită”, deoarece se concentrează pe persoane sau grupuri identificate. În prezentul raport, prin „supraveghere țintită” se înțelege monitorizarea deliberată a anumitor persoane sau grupuri de către serviciile de poliție sau de informații.[18]

14. În mod tradițional, supravegherea țintită implică multe resurse. Acest lucru pare încă a fi cazul pentru utilizarea programelor spion. Programele de tip spion exploatează deficiențe de securitate în anumite dispozitive sau aplicații, care sunt apoi utilizate pentru a oferi „hackerului” controlul asupra dispozitivului în sine.[19] Din motivul expertizei tehnice semnificative necesare, unele guverne achiziționează servicii de programe spion de la un operator comercial, care pot fi costisitoare.[20] Acestea fiind spuse, după cum a menționat Comisia de la Veneția în Lista sa de verificare a statului de drept, evoluțiile tehnice fac supravegherea „din ce în ce mai ușor de utilizat”. [21] Aceasta înseamnă că tehnologia de supraveghere devine accesibilă pentru o serie de state care ar putea să nu dispună de expertiză tehnică internă, precum și de garanții sistematice în domeniul drepturilor omului. Prin urmare, este esențial ca garanțiile stricte care respectă drepturile omului și statul de drept să se aplice dezvoltării și utilizării tehnologiilor precum sunt programele de tip spion, pentru a evita oferirea statelor a puterii de a interfera cu protecția și garanțiile necesare într-o societate democratică.

[15] A se vedea, de exemplu, *Citizen Lab, Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuous Proliferation*, 15 octombrie 2015; "*The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender"*, 24 august 2016; "*HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 septembrie 2018; *Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, 16 decembrie 2021; "*GeckoSpy: Pegasus Spyware Used against Thailand's ProDemocracy Movement*, 17 iulie 2022; "*PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions*", 22 septembrie 2023.

[16] A se vedea, de exemplu, *Amnesty Tech, Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 iulie 2021; *Dominican Republic: Pegasus spyware discovered on prominent journalist's phone*, 2 mai 2023; *Global: A Web of Surveillance – Unravelling a murky network of spyware exports to Indonesia*, 2 mai 2024.

[17] A se vedea, de exemplu,, *Access Now, Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict*, 25 mai 2023; *Hacking Meduza: Pegasus spyware used to target Putin's critic, 13 septembrie 2023; New spyware attacks exposed: civil society targeted in Jordan*, 1 februarie 2024; *Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware*, 30 mai 2024.

[18] Spre deosebire de supravegherea strategică sau „în masă”, care constă mai degrabă în colectarea generală a unor cantități foarte mari de date și metadate de conținut electronic care sunt apoi supuse analizei computerizate cu ajutorul selectoarelor.

[19] Aplicațiile sunt în mod normal concepute astfel încât să fie „sigilate” unele de altele. Chiar dacă o vulnerabilitate poate fi găsită, este posibil să nu poată fi exploatată suficient. S-ar putea să fie necesare „atacuri” repetate și chiar și atunci s-ar putea să nu aibă succes. Există adesea un element considerabil de șansă implicat dacă spyware-ul va fi sau nu eficient sau nu. Deoarece procesul real de executare de la distanță a spyware-ului va fi extrem de tehnic și de obicei consumator de mult timp, este nevoie de o echipă de specialiști pentru a face acest lucru.

[20] În 2016, s-a raportat că NSO a taxat agențiile guvernamentale cu 650.000 de dolari pentru a utiliza Pegasus pe zece ținte, plus o taxă de instalare de 500.000 de dolari

[21] Comisia de la Veneția, CDL-AD(2016)007, Lista criteriilor statului de drept, § 118.

15. Pe baza rezultatelor studiului comparativ privind cadrele juridice care reglementează utilizarea programelor spion în statele sale membre și bazându-se pe jurisprudența Curții Europene a Drepturilor Omului Drepturi (CEDO) în materia supravegherii țintite, Comisia de la Veneția a încercat să identifice garanțiile minime care ar trebui să fie stabilite atunci când este vorba de măsuri intruzive de supraveghere țintită, pentru a preveni practicile de supraveghere ilegală. Complexitatea cadrelor legislative în cauză, lipsa unor informații cuprinzătoare și practice privind punerea în aplicare a standardelor internaționale existente, cum ar fi articolul 9 din Convenția 108, precum și raritatea reglementărilor specifice programelor de tip spion au fost factori importanți de luat în considerare la pregătirea raportului. Exemplele menționate în raport nu sunt exhaustive și sunt prezentate doar în scopuri comparative. Faptul că acestea sunt menţionate nu înseamnă că Comisia de la Veneţia le susţine tacit ca fiind compatibile cu drepturile omului şi statul de drept. În cele din urmă, îi va reveni CEDO, în contextul examinării cauzelor legate de „programe spion”[22], să stabilească standardele minime aplicabile în acest domeniu. O contribuție importantă la definirea acestor standarde la nivel mondial poate fi, de asemenea, furnizată de Comitetul Convenției 108+ în cadrul lucrărilor sale privind interpretarea articolului 11 și al mecanismului de evaluare și monitorizare care urmează să fie implementat în temeiul Convenției 108+.

III. Jurisprudenţa Curții Europene a Drepturilor Omului şi alte standarde europene şi internaţionale privind programele spion[23]

A. Jurisprudența Curții Europene a Drepturilor Omului privind dreptul la respectarea vieții private și lucrările anterioare ale Comisiei de la Veneția

16. Nu se contestă faptul că datele cu caracter personal conținute într-un dispozitiv, inclusiv comunicațiile mobile/telefonice, sunt acoperite de noțiunile de „viață privată” și „corespondență”. Utilizarea programelor de tip spion interferează direct cu dreptul la respectarea vieții private, așa cum este consacrat la articolul 8 din Convenția Europeană a Drepturilor Omului (CEDO) și articolul 17 din Pactul internațional privind Drepturile Civile și Politice (PIDCP). O astfel de ingerință poate fi permisă numai în trei condiții: condițiile în care poate avea loc ingerința trebuie să fie definite în mod clar prin lege, într-o legislație sau reglementare care trebuie să fie accesibilă persoanei în cauză și să-l protejeze de arbitrariu, în special prin precizie și previzibilitate; ea trebuie să urmărească unul dintre scopurile legitime enumerate la articolul 8 § 2 din CEDO; [24] și trebuie să corespundă unei necesități sociale imperioase[25]și să fie proporțională cu scopul legitim urmărit, astfel încât să poată fi considerată necesară într-o societate democratică. Cele trei condiții enumerate mai sus sunt cumulative și fiecare are o funcție autonomă de îndeplinit. Igerințele

[22] A se vedea Curtea Europeană, Brejza c. Polonia și alte 8 (comunicare), nr. 27830/23 și alte 8, 3 iulie 2024; a se vedea, de asemenea, Koukakis v. Grecia (comunicare), nr. 37659/22, 10 ianuarie 2024; pentru un context faptic al cazului, a se vedea Raportul privind investigarea presupuselor încălcări și administrare defectuoasă în aplicarea dreptului Uniunii în legătură cu utilizarea Pegasus și a unui spyware de supraveghere echivalent (2022/2077(INI)) („Raportul PEGA”), 22 mai 2023, §§ 202-210 și Raportul APCE, citat mai sus, Expunerea de motive §§ 31-35. Cauza a fost în cele din urmă declarată inadmisibilă de Curtea Europeană din cauza abuzului de drept de aplicare, a se vedea Curtea Europeană, Koukakis v. Grecia (decizie), nr. 37659/22, 11 iunie 2024.

[23] O prezentare generală extinsă a standardelor existente și aplicabile ale Consiliului Europei și a standardelor internaționale se găsește în Raportul APCE, citat mai sus, Expunere de motive §§ 64-80.

[24] Sau, în cadrul PIDCP, să respecte prevederile, scopurile și obiectivele Pactului, a se vedea Oficiul Înaltului Comisar pentru Drepturile Omului, CCPR Comentariul general nr. 16: Articolul 17 din onoare și reputație, 8 aprilie 1988, § 3-4.

[25] Curtea Europeană, Dudgeon v. Regatul Unit, nr. 7525/76, 22 octombrie 1981, § 51.

disproporţionate în dreptul la respectarea vieţii private nu sunt compatibile cu Convenţia, chiar şi în scopul realizării unor obiective legitime şi foarte urgente.

17. În funcţie de circumstanţele cazurilor individuale, utilizarea programelor spion poate afecta şi alte câteva drepturi şi libertăţi ale omului (de exemplu, dreptul la un proces echitabil, libertatea religioasă, libertatea de exprimare, libertatea de întrunire și de asociere, libertatea de circulație, dreptul la alegeri libere, dreptul la nediscriminare,[26] dreptul de a nu fi supus unui tratament inuman sau degradant[27]) fie direct, fie printr-un „efect de răcire” care rezultă dintr-o intruziune de prim ordin în dreptul la viață privată, care afectează, de asemenea, respectul sau exercitarea de către persoane a celorlalte drepturi ale acestora.[28] În plus, programele spion pot afecta nu numai drepturile omului cu referire la ţintele directe, ci şi drepturile altor persoane, inclusiv ale copiilor, care intră în contact cu acestea. Dreptul la protecția vieții private (și dreptul la protecția datelor cu caracter personal, care este recunoscut ca un atribut important al dreptului la viața privată în jurisprudența Curții Europene) tinde să fie dreptul fundamental cel mai des şi cel mai direct afectat de utilizarea programelor spion, acest raport se concentrează asupra interferenţelor cu articolul 8 din CEDO.

18. Curtea Europeană trebuie încă să dezvolte o jurisprudență specifică asupra proporționalității utilizării programelor de tip spion. Cu toate acestea, ea a elaborat deja o jurisprudență substanțială în domeniul supravegherii în general, în care a stabilit o distincție între supravegherea țintită și interceptarea liberă.[29] În cauza *Roman Zaharov v. Rusia*, Marea Cameră a Curții a codificat următoarele garanții minime care trebuie să fie prevăzute în lege, atunci când este vorba de măsuri de supraveghere (secretă) țintită, pentru a evita abuzurile de putere: (i) o declarație clară a naturii infracțiunilor care pot determina un ordin de interceptare; (ii) o definiţie a

[26] Într-adevăr, pot apărea probleme atunci când supravegherea se bazează pe algoritmi sau pe alte metode de "profilare" a indivizilor pentru supraveghere țintită din cauza apartenenței lor la un grup rasial, etnic, cultural, religios, politic sau de altă natură. Crearea de profiluri nediscriminatorii într-un context de drept penal este, în principiu, un mijloc permis de activitate de aplicare a legii: profilurile detaliate bazate pe factori care s-au dovedit statistic că se corelează cu anumite comportamente infracționale pot fi instrumente eficiente pentru a direcționa mai bine resursele limitate de aplicare a legii. Cu toate acestea, o diferență de tratament bazată pe un criteriu precum rasa, etnia, originea națională sau religia nu va fi compatibilă cu principiul nediscriminării decât dacă este susținută de motive obiective și rezonabile. Astfel, diferența de tratament trebuie să urmărească un obiectiv legitim. În plus, trebuie să existe un raport rezonabil de proporționalitate între diferența de tratament și obiectivul legitim urmărit. Rezultă că, în cazul în care autoritățile de aplicare a legii utilizează profiluri largi care reflectă generalizări neexaminate, practicile lor de supraveghere țintită pot constitui ingerințe disproporționate în drepturile omului. În special, crearea de profiluri bazată pe presupuneri stereotipe conform cărora persoanele de o anumită "rasă", origine națională sau etnică sau religie sunt deosebit de susceptibile de a comite infracțiuni poate duce la practici incompatibile cu principiul nediscriminării. Dacă are loc țintirea selectivă, aceasta ar trebui să se bazeze pe comportamentul individual, nu pe caracteristicile înnăscute sau pe apartenența la un grup. A se vedea Agenția pentru Drepturi Fundamentale, Prevenirea creării ilegale de profiluri astăzi și în viitor: un ghid, 5 decembrie 2018, în special secțiunea 2 intitulată „Crearea de profiluri legale: principiu și practică”; a se vedea, de asemenea, Rețeaua UE de experți independenți în domeniul drepturilor fundamentale, crearea de profiluri etnice, decembrie 2006; Comisia Europeană împotriva Rasismului și Intoleranței, Recomandarea de politică generală nr. 11 a ECRI privind combaterea rasismului și a discriminării rasiale, 29 iunie 2007; Comitetul pentru eliminarea discriminării rasiale, Recomandarea generală nr. 36 (2020) privind prevenirea și combaterea profilării rasiale de către agenții de aplicare a legii, 17 decembrie 2020.

[27] În cel puțin o jurisdicție - Regatul Unit - s-a susținut că utilizarea programelor spion a cauzat victimei un prejudiciu psihiatric, astfel încât aceasta a fost exceptată de la imunitatea suverană și au putut fi inițiate proceduri civile împotriva statului străin presupus responsabil (a se vedea Al Masarir împotriva Regatului Arabiei Saudite [2023] 2 WLR 549, 19 august 2022; Shehabi împotriva Regatului Bahrain [2024] EWCA Civ 1158, 4 octombrie 2024).

[28] Consiliul Europei, Programul spion Pegasus și impactul său asupra drepturilor omului („Raportul DGI privind programele spion”), 2022, capitolul 5: „[...] Supravegherea țintită sau în masă creează, de asemenea, un climat de autocenzură. Temându-se că fiecare acțiune și mișcare este sub control, oamenii vor fi mai puțin predispuși să comunice despre anumite subiecte online sau offline. Efectul înfricoșător al supravegherii ar putea duce, de asemenea, la izolare socială. Țintele, precum și rudele și prietenii lor, s-ar putea abține de la interacțiuni de teama de a fi răniți sau supravegheați. Mai important, accesul în timp real la datele de localizare și comunicare ar putea reprezenta, de asemenea, un risc de viață pentru individ și i-ar pune în pericol integritatea fizică și mentală [...].”

[29] Pentru supravegherea țintită și secretă, a se vedea, printre multe altele, Curtea Europeană, Roman Zakharov v. Rusia [MC], nr. 47143/06, 4 decembrie 2015 ș iKennedy v. Regatul Unit, nr. 26839/05, 18 mai 2010; pentru interceptarea în masă, a se vedea Curtea Europeană, Big Brother Watch și alții v. Regatul Unit [MC], nr. 58170/13 și 2 alții, 25 mai 2021 și Centrum För Rättvisa v. Suedia [MC], nr. 35252/08, 25 mai 2021.

categoriilor de persoane susceptibile de a fi ascultate; (iii) o limită a duratei interceptării; (iv) procedura care trebuie urmată pentru examinarea, utilizarea și stocarea datelor obținute; (v) măsurile de precauție care trebuie luate la comunicarea datelor către alte părți; și (vi) circumstanțele în care înregistrările pot sau trebuie să fie șterse sau distruse.[30] În aceeași hotărâre, CEDO a stabilit, de asemenea, o obligație generală de notificare retroactivă, sub rezerva unor excepții.[31] Aplicând jurisprudența menționată mai sus, CEDO a evaluat recent legislația națională poloneză privind supravegherea secretă și a constatat trei încălcări separate ale articolului 8 CEDO.[32]

19. În schimb, supravegherea în masă le permite serviciilor de securitate să adopte o abordare proactivă prin căutarea pericolelor necunoscute anterior, mai degrabă decât prin investigarea celor cunoscute. Curtea Europeană s-a ocupat de problema interceptării în masă în cauzele istorice *Big Brother Watch și alții v. Regatul Unit* [MC] și *Centrum För Rättvisa v. Suedia* [GC]. Curtea Europeană a constatat că interceptarea în masă este „o capacitate tehnologică valoroasă pentru a identifica noi amenințări în domeniul digital”[33] și că este de o importanță vitală pentru statele contractante în identificarea amenințărilor la adresa securității lor naționale.[34] Deși articolul 8 din CEDO nu interzice utilizarea interceptării în masă pentru a proteja securitatea națională și alte interese naționale esențiale împotriva amenințărilor externe grave, iar statele se bucură de o largă marjă de apreciere în a decide ce tip de regim de interceptare este necesar, în aceste scopuri, marja discreționară care le este acordată în cadrul implementării unui astfel de sistem trebuie să fie în mod necesar redusă și mai multe garanții vor trebui stabilite.[35]

20. Pe baza jurisprudenței Curții Europene, se observă că, în pofida diferențelor, în practică pot exista mai multe suprapuneri între interceptarea țintită și cea în masă. Orice intruziune cauzată de achiziționarea datelor de comunicații asociate este multiplicată de interceptarea în masă, deoarece astfel de date pot fi deja analizate și cercetate, ceea ce permite realizarea unui portret intim al persoanei în cauză prin urmărirea activităților sale pe rețelele de socializare, a deplasărilor sale, a obiceiurilor sale de navigare pe internet și de comunicare, precum și a contactelor sale.[36] Datele în vrac pot fi analizate pentru a identifica dispozitivele individuale care prezintă un interes, care pot face apoi obiectul unei interceptări țintite.

21. Comisia de la Veneţia a luat în considerare, de asemenea, probleme de supraveghere. În 2015, Comisia și-a actualizat Raportul privind controlul democratic al serviciilor de securitate[37]și a elaborat un raport privind controlul democratic al

[30] Curtea Europeană, Roman Zakharov v. Rusia [MC], citată mai sus, § 231.
[31] Ibid., §§ 286 et ff., a se vedea secțiunea V.H de mai jos.
[32] Curtea Europeană, Pietrzak și Bychawska-Siniarska și alții v. Polonia, nr. 72038/17 și 25237/18, 28 mai 2024.
[33] Curtea Europeană, Big Brother Watch și alții v. Regatul Unit [MC], citată mai sus, § 323
[34] Ibidem, § 424; a se vedea, de asemenea, Comisia de la Veneția, CDL-AD(2015)011, Raport privind supravegherea democratică a agenților de informații de origine electromagnetică, § 47.
[35] Curtea Europeană, Big Brother Watch și alții v. Regatul Unit [MC], citată mai sus § 347. În special, Curtea a examinat dacă cadrul juridic intern a definit în mod clar: (i) motivele pentru care poate fi autorizată interceptarea în masă; (ii) circumstanțele în care comunicațiile unei persoane pot fi interceptate; (iii) procedura care trebuie urmată pentru acordarea autorizației; (iv) procedurile care trebuie urmate pentru selectarea, examinarea și utilizarea materialelor interceptate; (v) măsurile de precauție care trebuie luate atunci când comunică materialul altor părți; (vi) limitele privind durata interceptării, depozitarea materialului interceptat și circumstanțele în care aceste materiale trebuie șterse și distruse; (vii) procedurile și modalitățile de supraveghere de către o autoritate independentă a respectării garanțiilor menționate mai sus și competențele acesteia de a aborda neconformitatea; (viii) procedurile de examinare independentă a posteriori a unei astfel de conformități și competențele cu care este învestit organismul competent în soluționarea cazurilor de neconformitate, a se vedea para. 361.
[36] Curtea Europeană, Pietrzak și Bychawska-Siniarska și alții v. Polonia, citată mai sus, § 249.
[37] Comisia de la Veneția, CDL-AD(2015)010, Raport privind supravegherea democratică a serviciilor de securitate.

agențiilor de informații de origine electromagnetică.[38] Prin urmare, prezentul raport ar trebui citit împreună cu aceste rapoarte, care vor fi menționate în secțiunea V. Comisia de la Veneția a adoptat, de asemenea, opinii privind legile referitoare la supravegherea țintită.[39]

B. Protecția datelor cu caracter personal

22. Deși dreptul la protecția datelor cu caracter personal nu este un drept autonom în temeiul CEDO, Curtea Europeană a recunoscut că protecția datelor cu caracter personal este de o importanță fundamentală pentru exercitarea de către o persoană a dreptului său la respectarea vieții private și de familie, a domiciliului și a corespondenței.[40]

23. Convenţia Consiliului Europei 108,[41] singurul tratat internațional obligatoriu din punct de vedere juridic în domeniul protecției datelor cu caracter personal cu relevanță mondială stabilește principiile de bază pentru protecția datelor, garanțiile pentru persoane și controlul operațiunilor de prelucrare a datelor, care sunt deosebit de importante în contextul tehnologiilor de supraveghere, cum ar fi programele de tip spion.[42] Convenția 108+ modernizată[43] a fost deschisă pentru semnături și ratificări în octombrie 2018.[44]

1. *Principalele exigențe ale Convenției 108+*

24. Convenția 108+ stabilește cerințe mai stricte privind legalitatea prelucrării, necesitatea, proporționalitatea, limitarea scopului, calitatea datelor și minimizarea datelor, reamintind că datele cu caracter personal prelucrate trebuie să fie adecvate, relevante, și nu excesiv. Principiul proporționalității se aplică, de asemenea, în ceea ce privește mijloacele și metodele utilizate în timpul supravegherii. Convenția 108+ le oferă persoanelor un control mai mare asupra datelor lor personale și drepturi consolidate.[45] În plus, se precizează că exigența unui temei juridic valabil pentru prelucrare se aplică în toate circumstanțele, fără excepție. Printre alte obligații, responsabilii prelucrării trebuie să implementeze principiile de „confidențialitate prin design” și „confidențialitate implicită” în dezvoltarea de produse sau servicii [46] și

[38] CDL-AD(2015)011, citată mai sus.
[39] A se vedea, printre altele, Comisia de la Veneția, CDL-AD(2016)012, Polonia – Aviz referitor la Legea din 15 ianuarie 2016 de modificare a Legii privind poliția și a altor acte.
[40] Curtea Europeană, Satakunnan Markkinapörssi Oy și Satamedia Oy v. Finlanda, nr. 931/13, 27 iunie 2017, § 137.
[41] Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal (ETS nr. 108)
[42] Raportul DGI privind programele spion, citat mai sus, p. 14.
[43] Convenția pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, astfel cum va fi modificată prin Protocolul său CETS Nr. 223.
[44] 31 de țări au ratificat până în prezent Protocolul de modificare a Convenției 108. Convenția modernizată va intra în vigoare după ratificarea de către toate cele 55 de părți la Convenția 108 sau, începând cu 11 octombrie 2023, după ratificarea protocolului de către 38 de părți la convenție
[45] La articolul 9, convenția modernizată extinde catalogul de informații care trebuie transmise persoanelor vizate atunci când își exercită dreptul de acces. În plus, persoanele vizate au dreptul de a lua cunoștință de raționamentul care stă la baza prelucrării datelor, ale căror rezultate sunt aplicate în cazul lor/ei. Dreptul de a nu fi supus unei decizii care afectează în mod semnificativ persoana vizată care se bazează exclusiv pe o prelucrare automată, fără ca persoana vizată să aibă în vedere opiniile sale. În sfârșit, persoanele vizate au dreptul de a se opune în orice moment prelucrării datelor lor cu caracter personal, cu excepția cazului în care operatorul demonstrează motive legitime imperioase pentru prelucrare care prevalează asupra intereselor sau drepturilor și libertăților lor fundamentale, a se vedea, de asemenea, Consiliul Europei, Convenția 108 modernizată: noutățile pe scurt.
[46] Conceptul de „privacy by design”, conform căruia protecția vieții private a fiecărui utilizator trebuie să înceapă în etapa de proiectare a sistemelor informatice. Acesta a fost codificat prin Regulamentul (UE) 2016/679 (GDPR). Permite protecția maximă a drepturilor privind datele cu caracter personal încă din faza de proiectare și în timpul fiecărei utilizări a unei noi tehnologii. Principiul presupune că protecția datelor cu caracter personal nu mai este o opțiune pentru întreprinderi, ci o obligație inerentă fiecăreia dintre activitățile lor.

trebuie să efectueze o examinare prospectivă a impactului probabil al prelucrării datelor asupra drepturilor omului și a libertăților fundamentale.

25. O exigență-cheie a Convenției 108+ și a noii generații de legi privind protecția datelor este ca operatorii de date cu caracter personal (inclusiv serviciile de informații și poliția) și, după caz, procesatorii de date (inclusiv dezvoltatorii și furnizorii de servicii) trebuie să poată demonstra că prelucrarea datelor cu caracter personal sub controlul lor respectă principiile (inclusiv legalitatea, limitarea scopului, minimizarea datelor, limitările de stocare, calitatea datelor) și obligațiile prevăzute în Convenție, inclusiv respectarea vieţuu private de la concepere, respectarea vieții private în mod implicit și evaluarea impactului asupra protecției datelor. În plus, articolul 6 din Convenția 108+ prevede că datele cu caracter personal care dezvăluie originea rasială, opiniile politice sau convingerile religioase sau de altă natură, precum și datele cu caracter personal privind sănătatea sau viața sexuală, nu pot fi procesate automat decât dacă legislația națională prevede garanții adecvate. Același lucru se aplică datelor cu caracter personal referitoare la condamnările penale. Astfel, această dispoziție limitează efectiv utilizarea directă a criteriilor enumerate în practicile de supraveghere, deși utilizarea unor astfel de criterii în supraveghere nu este întotdeauna interzisă. De exemplu, aceste criterii pot fi aplicate supravegherii țintite în cazul în care există informații specifice care sugerează că o persoană identificabilă care îndeplinește aceste caracteristici pregătește o infracțiune gravă specifică sau un act care reprezintă o amenințare gravă la adresa securității naționale.

26. Evaluarea impactului asupra vieții private (EIVP) prevăzută la articolul 10 § 2 din Convenția 108+ este esențială în contextul programelor spion, întrucât este un proces conceput pentru a descrie prelucrarea datelor cu caracter personal, pentru a evalua necesitatea și proporționalitatea acesteia, să identifice impactul prelucrării urmărite a datelor asupra drepturilor și libertăților fundamentale ale persoanelor vizate și să atenueze riscurile care decurg din prelucrare. O analiză a impactului nu trebuie neapărat să indice faptul că toate riscurile au fost eradicate, ci ar trebui să reducă la minimum riscurile cât de mult și rapid posibil și să evalueze dacă riscurile reziduale sunt justificate.

27. Exigența potrivit căreia motivele pentru care este permisă prelucrarea datelor cu caracter personal să fie stabilite în mod clar și precis de lege este unul dintre principiile fundamentale referitoare la protecția datelor cu caracter personal date personale. Exigența de „calitate” a legii poate fi derivată și din articolul 11 din Convenția 108+, în măsura în care aceasta prevede în mod explicit că excepțiile și restricțiile să fie „prevăzute de lege”.[47]

28. Din aceste cerințe rezultă că legislația care le oferă autorităților puterea de a interfera cu viața privată și datele cu caracter personal prin utilizarea programelor spion și apoi prelucrarea ulterioară a datelor cu caracter personal obținute prin utilizarea programelor spion trebuie să conțină dispoziții explicite și detaliate privind persoanele autorizate să consulte datele, natura și categoria datelor, procedura care trebuie urmată sau utilizarea care poate fi făcută a informațiilor astfel obținute. Cerința unor dispoziții legale explicite și suficient de detaliate și precise constituie,

[47] Paragraful 91 din Raportul explicativ al Convenției 108+ precizează, de asemenea, că „o astfel de măsură trebuie să fie prevăzută de o lege accesibilă și previzibilă, care trebuie să fie suficient de detaliată”.

de asemenea, o garanție esențială împotriva arbitrarului și a abuzului de putere, care este de o importanță deosebită în ceea ce privește utilizarea programelor spion, datorită potențialului sporit de ingerință intruzivă a acestor tehnologii de supraveghere.

2. *Securitatea națională și protecția datelor cu caracter personal*

29. Spre deosebire de dispozițiile Convenției 108, Convenția 108+ nu mai permite excluderea în totalitate din câmpul de aplicare al Convenției prelucrarea datelor din motive legate de Securitate (și apărarea) națională (articolul 11). Eventualele excepții de la un număr limitat de principii (articolul 5 alin. (4), articolul 7 (2), articolul 8 (1) și articolul 9), sunt supuse condiţiilor stabilite de Convenţie. Anume, astfel de excepții trebuie: (i) să fie prevăzute de lege; (ii) să respecte esența drepturilor și libertăților fundamentale și (iii) constituie o măsură necesară într-o societate democratică pe baza unor motive specificate și limitate, inclusiv „protecția securității naționale, a apărării, a siguranței publice, interesele economice și financiare importante ale statului, imparțialitatea și independența sistemului judiciar sau prevenirea, investigarea și urmărirea infracțiunilor penale și executarea pedepselor penale, alte obiective esențiale de interes public general”.

30. De asemenea, în temeiul articolului 11 § 3, activitățile de prelucrare în scopuri de securitate națională și apărare ar trebui să facă obiectul unei examinări și al unui control independent și efectiv în temeiul legislației interne a statului Parte respectiv.

C. Activitatea instituțiilor și tribunalelor internaționale în materia programelor de tip spion

31. Pe lângă activitatea desfășurată de APCE, o examinare amănunțită a utilizării programului Pegasus și a altor programe spion a fost efectuată de Parlamentul European, care a creat o comisie de anchetă privind utilizarea programului Pegasus și a programelor spion echivalente de supraveghere (Comisia PEGA).[48] Comisia a elaborat un studiu privind utilizarea Pegasus şi a programelor spion de supraveghere echivalente,[49] un raport [50] și o recomandare adresată Consiliului European și Comisiei.[51] În 2019, Raportorul special al Organizației Națiunilor Unite privind promovarea și protecția dreptului la libertatea de opinie și de exprimare a publicat un raport privind supravegherea și drepturile omului, care a făcut referire la programul spion Pegasus ca un exemplu de piratare al dispozitivelor mobile folosit ca instrument de supraveghere țintită în 45 de țări.[52] În 2022, Comisarul ONU pentru Drepturile Omului a constatat că utilizarea programelor spion „*ar trebui să se limiteze la cazurile în care ar servi la prevenirea sau investigarea unei infracțiuni grave*

[48] Parlamentul European, Decizia din 10 martie 2022 privind înființarea unei comisii de anchetă pentru a investiga utilizarea Pegasus și a programelor spion de supraveghere echivalente și definirea obiectului anchetei, precum și a responsabilităților, a componenței numerice și a duratei de mandat a comisiei (2022/2586(RSO)), 10 martie 2022.
[49] Studiul PEGA, citat mai sus.
[50] Raportul PEGA, citat mai sus.
[51] Recomandarea Parlamentului European din 15 iunie 2023 adresată Consiliului și Comisiei în urma investigării presupuselor încălcări și administrare defectuoasă în aplicarea dreptului Uniunii în ceea ce privește utilizarea Pegasus și a unui spion de supraveghere echivalent (2023/2500(RSP)) („Recomandarea PE”).
[52] Adunarea Generală a Organizației Națiunilor Unite, Consiliul pentru Drepturile Omului, A/HRC/41/35, Raportul Raportorului special privind promovarea și protecția dreptului la libertatea de opinie și de exprimare („Raportul SR al ONU din 2019”), 28 mai 2019. A se vedea, de asemenea, Raportorul special al Organizației Națiunilor Unite pentru promovarea și protecția drepturilor omului și a libertăților fundamentale în combaterea terorismului, Reglementarea globală a comerțului cu tehnologie spyware de combatere a terorismului : propuneri de definire a domeniului de aplicare pentru o abordare conformă cu drepturile omului (aprilie 2023).

specifice sau a unui act care reprezintă o amenințare gravă la adresa securității naționale. Utilizarea sa ar trebui să vizeze strict o investigație a persoanei sau a persoanelor suspectate de comiterea sau că au comis astfel de acte. Aceasta ar trebui să fie o măsură de ultim resort [.] toate măsurile mai puțin intruzive ar fi trebuit să fie epuizate sau să se dovedească a fi inutile și ar trebui să fie strict limitate în ceea ce privește domeniul de aplicare și durata. Trebuie accesate și colectate numai datele relevante. Măsurile ar trebui, de asemenea, să facă obiectul unui control independent riguros, și supusă unei aprobări prealabile de către un organism judiciar. [...]”[53] În 2023, Comisarul pentru Drepturile Omului al Consiliului Europei a publicat un comentariu în care le solicita statelor membre ale Consiliului Europei să impună un moratoriu strict asupra exportului, vânzării, transferului, și utilizării programelor de tip spion extrem de intruzive cu zero-click, cum ar fi Pegasus, și să implementeze un cadru legislativ precis și care respectă drepturile omului pentru utilizarea tehnologiei moderne de supraveghere.[54]

32. Alte materiale relevante, printre altele, includ raportul actualizat al Agenției pentru Drepturi Fundamentale din 2023 privind „Supravegherea de către serviciile de informații”, [55] care a actualizat parțial rapoartele din 2015 și 2017 ale aceleiași agenții și oferă o examinare cuprinzătoare a mecanismelor de control existente în țările UE și raportul Consiliului Europei din 2022 privind programul spion Pegasus și impactul acestuia asupra drepturilor omului.[56]

33. În 2024, Lagea europeană pentru libertatea presei, menționată anterior, în considerentele sale 25 și 26, a stabilit anumite garanții care trebuie respectate pentru a permite utilizarea legală a programelor de supraveghere intruzivă împotriva furnizorilor de servicii media.[57] Articolul 4 § 3 din Lege, în conformitate cu protecția largă a jurnaliștilor recunoscută de dreptul internațional al drepturilor omului în

[53] Consiliul pentru Drepturile Omului, Dreptul la viață privată în era digitală, Raportul Oficiului Înaltului Comisar al Națiunilor Unite pentru Drepturile Omului, A/HRC/51/17, 4 august 2022

[54] Consiliul Europei, comisar pentru drepturile omului, Un program spion extrem de intruziv amenință esența drepturilor omului, 27 ianuarie 2023.

[55] Raportul FRA, citat mai sus.

[56] Raportul DGI privind programele spin, citat mai sus, p. 14.

[57] Considerentele (25) și (26) Programul de supraveghere intruzivă, care include în special ceea ce este denumit în mod obișnuit «spyware», reprezintă o formă deosebit de invazivă de supraveghere a profesioniștilor din mass-media și a surselor acestora. Acesta poate fi utilizat pentru a înregistra în secret apeluri sau pentru a utiliza în alt mod microfonul unui dispozitiv al utilizatorului final, pentru a filma sau fotografia persoane fizice, mașini sau împrejurimile acestora, pentru a copia mesaje, pentru a accesa date de conținut criptate, pentru a urmări activitatea de navigare, pentru a urmări geo-localizarea sau pentru a colecta alte date ale senzorilor sau pentru a urmări activitățile pe mai multe dispozitive ale utilizatorilor finali. Aceasta are efecte disuasive asupra liberei exercitări a activităților economice în sectorul mass-mediei. Aceasta pune în pericol, în special, relația de încredere a jurnaliștilor cu sursele lor, care este nucleul profesiei jurnalistice. Având în vedere caracterul digital și intruziv al unui astfel de software și utilizarea transfrontalieră a dispozitivelor, acesta are un impact deosebit de negativ asupra exercitării activităților economice de către furnizorii de servicii mass-media pe piața internă. Prin urmare, este necesar să se asigure că furnizorii de servicii mass-media, inclusiv jurnaliștii, care își desfășoară activitatea pe piața internă a serviciilor mass-media se pot baza pe o protecție armonizată solidă în ceea ce privește implementarea unui software de supraveghere intruziv în Uniune, inclusiv în cazul în care autoritățile statelor membre recurg la părți private pentru a-l implementa; (26) Software-ul de supraveghere intruzivă ar trebui să fie utilizat numai în cazul în care este justificat de un motiv imperativ de interes public, este prevăzut de dreptul Uniunii sau de dreptul intern, este în conformitate cu articolul 52 alineatul (1) din cartă, astfel cum a fost interpretat de Curtea de Justiție și cu alte tipuri de drept al Uniunii, a fost autorizat ex ante sau, în cazuri excepționale și urgente, confirmate ulterior de o autoritate judiciară sau de o autoritate decizională independentă și imparțială, aceasta apare în cadrul anchetelor privind infracțiunile enumerate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului (9), care se pedepsesc în statul membru în cauză cu o pedeapsă privată de libertate sau cu o măsură de siguranță privative de libertate cu o perioadă maximă de cel puțin trei ani sau în cadrul anchetelor privind alte infracțiuni grave care se pedepsesc în statul membru în cauză cu o pedeapsă privativă de libertate o pedeapsă sau o măsură de siguranță cu o durată maximă de cel puțin cinci ani, astfel cum este stabilită de dreptul intern al statului membru respectiv, și cu condiția ca nicio altă măsură mai puțin restrictivă să nu fie adecvată și suficientă pentru a obține informațiile solicitate. Potrivit principiului proporționalității, drepturile și libertățile unei persoane nu pot fi restrânse decât dacă acestea sunt necesare și răspund efectiv obiectivelor de interes general recunoscute de Uniune. Astfel, în ceea ce privește în mod specific utilizarea programelor informatice de supraveghere intruzivă, este necesar să se verifice dacă infracțiunea în cauză atinge un prag de gravitate prevăzut în prezentul regulament, dacă, în urma unei evaluări individuale a tuturor circumstanțelor relevante într-un anumit caz, este posibil ca cercetarea și urmărirea penală a infracțiunii respective”

calitate de „câine de pază” public al societății democratice, prevede standardul implicit conform căruia statele membre trebuie să asigure protecția surselor jurnalistice și a comunicațiilor confidențiale și să nu implementeze programe de tip spion împotriva furnizorilor de servicii media sau alții care ar putea implica divulgarea surselor și a comunicațiilor. Articolul 4 § 5 prevede derogări de la această protecție standard, și anume pentru instalarea de programe intruzive de supraveghere, numai în circumstanțe specifice (a se vedea paragraful 95 de mai jos).

34. Curtea de Justiție a Uniunii Europene (CJUE) a abordat, de asemenea, utilizarea tehnologiilor de supraveghere și impactul acestora asupra drepturilor fundamentale într-o serie de cazuri de referință[58].

IV. Constatări comparative privind legislația și practica în materia programelor de tip spion

35. În vederea realizării unui studiu comparativ privind cadrul legislativ al statelor sale membre privind utilizarea programelor spion, comisia de la Veneția s-a bazat pe garanțiile care au fost elaborate de Curtea Europeană în jurisprudența sa privind supravegherea țintită.[59] În special, ea l-ea solicitat membrilor săi să furnizeze informații cu privire la următoarele aspecte: (i) dacă cadrele juridice interne permit utilizarea programelor spion ca instrument de supraveghere țintită în cadrul anchetelor penale sau de informații; (ii) dacă există norme specifice (care acoperă în special domeniul de aplicare *ratione materiae, temporis* și *personae*) sau dacă se aplică normele generale privind supravegherea direcționată (interceptarea comunicațiilor); (iii) tipul de date, după caz, care ar putea fi colectate cu ajutorul programelor spion; (iv) existența unei evaluări oficiale a necesității sau a valorii adăugate a programelor spion; (v) organele responsabile de autorizarea/aprobarea măsurilor de supraveghere direcționată în cadrul anchetelor penale și de informații; (vi) mecanismele naționale de control instituite pentru activitățile serviciilor de securitate; și (vii) existența unui mecanism de notificare post-supraveghere sau a oricăror alte remedii.

36. Exemplele raportate nu sunt exhaustive și se bazează numai pe datele disponibile, în special pe răspunsurile furnizate la chestionar și pe informațiile care au fost colectate în alt mod de către raportori. În plus, Comisia de la Veneția

[58] Printre altele, CJUE, Digital Rights Ireland și Seitlinger și alții, cauzele conexate C-293/12 și C-594/12, 8 aprilie 2014; Tele2 Sverige AB/Post- och telestyrelsen și Secretary of State for the Home Department/Tom Watson și alții, cauzele conexate C-203/15 și C-698/15, 21 decembrie 2016; Maximillian Schrems împotriva Comisarului pentru protecția datelor, cauza C-362/14, 6 octombrie 2015; Privacy International/Secretary of State for Foreign and Commonwealth Affairs și alții, cauza C-623/17, 6 octombrie 2020; La Quadrature du Net și alții/Premier ministre și alții, cauzele conexate C-511/18, C-512/18 și C-520/18, 6 octombrie 2020. Rapoartele FRA din 2015, 2017 și 2023 includ liste cuprinzătoare ale hotărârilor judecătorești ale CJUE cu privire la aspecte legate de supraveghere. O hotărâre recentă a Marii Camere a CJUE (CG împotriva Bezirkshauptmannschaft Landeck, cauza C-548/21, 4 octombrie 2024) s-a referit la accesul poliției la datele conținute într-un telefon mobil, o ingerință conexă, dar mai puțin intruzivă, în implementarea unui software de supraveghere intruzivă. Deși a recunoscut că datele cu caracter personal stocate pe un telefon mobil pot constitui o ingerință deosebit de gravă în drepturile fundamentale ale persoanei vizate, Curtea a constatat că a considera că numai lupta împotriva infracțiunilor grave este de natură să justifice accesul la datele conținute într-un telefon mobil ar limita în mod nejustificat competențele de investigare ale autorităților competente. Acest lucru ar duce la un risc crescut de impunitate pentru infracțiunile în general și, prin urmare, la un risc pentru crearea unui spațiu de libertate, securitate și justiție în Uniunea Europeană. Cu toate acestea, Curtea a constatat că o astfel de ingerință în viața privată și în protecția datelor trebuie să fie prevăzută de lege, ceea ce implică faptul că legiuitorul național trebuie să definească elementele care trebuie luate în considerare pentru un astfel de acces, precum natura sau categoriile infracțiunilor în cauză. Pentru a asigura respectarea principiului proporționalității în fiecare caz specific, accesul la date trebuie să fie supus autorizării prealabile a unei instanțe sau a unei autorități independente, cu excepția cazurilor de urgență justificate în mod corespunzător. În sfârșit, persoana vizată trebuie să fie informată cu privire la motivele autorizării de îndată ce furnizarea acestor informații nu mai este susceptibilă să pună în pericol investigațiile.

[59] A se vedea para. 18 de mai sus.

reiterează faptul că exemplele citate în raport sunt prezentate doar în scopuri comparative și nu pentru a aproba o abordare anumită.

A. Baza legală de utilizare a programelor spion ca instrument de supraveghere țintită

37. Pe baza garanțiilor menționate mai sus, Comisia de la Veneția a examinat în primul rând cadrul juridic existent pentru utilizarea programelor spion în statele sale membre. S-a constatat că relativ puține state au elaborat o legislație care reglementează în mod specific utilizarea instrumentelor de supraveghere intruzivă/programe spion: **Canada, Danemarca, Finlanda, Germania, Italia, Luxemburg, Țările de Jos, Norvegia, Spania, Suedia, Elveția și Regatul Unit.** În **Austria**, legislația privind utilizarea programelor spion a fost introdusă inițial în contextul anchetelor penale. Cu toate acestea, ea a fost ulterior anulată de Curtea Constituțională care a considerat că aceasta constituie o ingerință disproporționată în drepturile omului.[60] În unele dintre statele menționate mai sus, au fost instituite norme specifice (*ratione materiae, ratione personae* și *ratione temporis*), care se abat de la cadrul general în vigoare pentru măsurile de supraveghere țintită (a se vedea mai jos secțiunea IV.C). În **Belgia, Bulgaria, Estonia, Franța, Ungaria, Lituania, Republica Moldova, Macedonia de Nord, Polonia, România** și **Republica Slovacă**, deși nu este reglementată separat și autonom, utilizarea programelor spion ar fi permisă în conformitate cu noțiunea de „mijloace tehnice speciale/măsuri speciale de investigare". În cazul statelor în care nu există o legislaţie specifică privind programele spion, pe baza informaţiilor disponibile, în cazul în care utilizarea programelor spion nu este *prima facie* interzisă în mod expres, este posibil ca normele generale privind supravegherea țintită să se aplice, iar programele spion să fie considerate ca o metodă care permite obținerea unor date relevante, fără norme specifice. Deși nu este reglementată în mod specific, jurisprudența tribunalelor din **Statele Unite** demonstrează că utilizarea internă a oricărei tehnologii de supraveghere ar trebui să fie reglementată de cerințe stricte privind mandatul, iar utilizarea acesteia ar trebui să aibă un domeniu de aplicare restrâns[61].

38. Legislația în vigoare în țările care reglementează în mod specific programele spion precede în mare parte dezvăluirile „Pegasus". Numai în **Grecia** a fost introdusă o legislaţie specifică în urma dezvăluirilor privind utilizarea abuzivă a programelor spion, stabilind, printre altele, un nou cadru juridic pentru ridicarea confidențialității

[60] A se vedea para. 70 de mai jos

[61] Al patrulea amendament al Constituției Statelor Unite oferă fundamentul cadrului legal american care guvernează supravegherea în sistemul de justiție penală. O decizie de referință este Curtea Supremă din 2018 Carpenter v. Statele Unite, care a găsit neconstituțională utilizarea fără mandat a informațiilor de localizare a site-urilor celulare, oferind astfel persoanelor protecție împotriva guvernului care caută date personale de la terți. Carpenter a furnizat un set de factori pentru a evalua constituționalitatea unor astfel de practici de supraveghere atunci când sunt efectuate fără un mandat judiciar, inclusiv factori de relevanță deosebită pentru spyware, cum ar fi, printre altele, natura revelatoare a informațiilor colectate și cantitatea de date solicitate de guvern. Instanțele inferioare au constatat că protecțiile celui de-al patrulea amendament constrâng utilizarea de către guvern a tehnologiilor care pot fi similare cu spyware-ul, așa cum sunt definite mai sus. De exemplu, în Statele Unite v. Wilson, Curtea de Apel a SUA pentru al nouălea circuit a constatat că instalarea de către forțele de ordine a malware-ului de supraveghere pe computerul unui inculpat fără mandat a fost o percheziție și confiscare ilegală. În Statele Unite v. Instanțele din Saboonchi au susținut că utilizarea de către forțele de ordine a malware-ului pentru a activa de la distanță camera web a laptopului inculpatului a fost o percheziție neconstituțională. Aceste cazuri conduc la concluzia că spyware-ul, având în vedere caracterul său intruziv, ar fi probabil guvernat strict de cerințele de garanție și de domeniul de utilizare. Acestea fiind spuse, aplicabilitatea legii în general la supravegherea digitală ar putea fi într-un anumit schimb. De exemplu, o curte de apel în Tuggle v. Statele Unite a constatat că utilizarea pe termen lung a unei camere de supraveghere pentru a monitoriza casa unei persoane este rezonabilă în conformitate cu al patrulea amendament.

comunicațiilor și autorizând achiziționarea programelor spion de către autoritățile statului.[62]

39. În statele în care utilizarea programelor spion este reglementată în mod explicit, în mod normal, acestea pot fi utilizate atât de către agenții repsonsabili de aplicarea legii în contextul anchetelor penale, cât și de către agențiile de securitate în contextul anchetelor de informații care urmăresc prevenirea amenințărilor la adresa securității naționale.[63] Uneori, autorizația legală de a utiliza programe spion poate fi găsită în aceeași lege, uneori în legi distincte.

40. Printre statele care permit utilizarea programelor spion, nu sunt disponibile date cu privire la instrumentul exact pe care îl utilizează autoritățile,[64] în special, dacă sunt utilizate programe spion comerciale sau dacă statul și-a dezvoltat propriile instrumente. Este posibil ca statele cu o vastă experiență și resurse în domeniul informației de origine electromagnetică să-și fi dezvoltat propriile instrumente. Pe baza răspunsurilor primite, Comisia de la Veneția a putut observa următoarele: în **Țările de Jos**, Centrul de Cercetare și Date al Ministerului Justiției și Securității din Țările de Jos a publicat un raport de evaluare privind competențele de supraveghere ale autorităților de aplicare a legii din Țările de Jos; acest raport a clarificat faptul că poliția olandeză a folosit un instrument comercial în „marea majoritate" a cazurilor. Cu toate acestea, denumirea instrumentului comercial nu este public. În **Elveția**, Tribunalul Administrativ Federal, printr-o hotărâre din 9 ianuarie 2022,[65] statuând asupra recursului unui avocat care a solicitat accesul la contractul privind programul spion utilizat de Oficiul Federal al Poliției și Serviciul de Informații al Confederației, a declarat că există un interes public important pentru a determina dacă programul achiziționat de Elveția este Pegasus. Curtea a considerat că cunoașterea informațiilor solicitate ar putea pune în pericol măsurile luate de Elveția în cazul unei amenințări concrete la adresa securității sale interne și externe, ceea ce, la rândul său, ar împiedica activitatea autorităților de aplicare a legii.

B. Tipul de informații care pot fi colectate prin intermediul programelor spion

41. Comisia de la Veneția a colectat în continuare informații cu privire la tipul de date care pot fi colectate prin intermediul programelor spion în țările care le reglementează în mod specific. În **Canada**, datele care pot fi colectate sunt limitate la comunicațiile private, la datele de transmisie și/sau la achiziționarea de date statice de pe dispozitive electronice. În **Danemarca**, legea nu stabilește nicio limitare specifică în acest sens. În **Finlanda**, legea nu permite supravegherea tehnică pentru

[62] Utilizarea programului spion de către agențiile de stat poate fi permisă, în condițiile unui decret prezidențial care nu a fost emis până în prezent (articolul 13 din legea 5002 din 2022).
[63] În Italia, legea nu face nicio referire explicită la posibilitatea de a utiliza spyware ca mijloc de interceptare a informațiilor; Cu toate acestea, unii autori, prin interpretare, permit această posibilitate; în Norvegia, Serviciul de Informații nu poate utiliza supravegherea țintită sau alte tipuri de supraveghere a persoanelor din Norvegia; în Spania, nu există o reglementare specifică privind utilizarea oricărui spyware (inclusiv Pegasus) de către serviciile de informații.
[64] Deși în țările în care este utilizat, programul spion este numit cu denumiri diferite: software/program în Finlanda (secțiunea 42 din Legea privind măsurile coercitive și secțiunea 42 din Legea privind informațiile militare), Norvegia (articolul 216 p din Legea de procedură penală) și Spania (capitolul IX, titlul VIII din Codul de procedură penală); interceptor informatic în Italia („captatore informatico", astfel cum este definit la articolul 1 litera (m) din Decretul ministerial din 6 octombrie 2022 ca "orice sistem deghizat, inoculat de la distanță, care, prin eliminarea efectelor care împiedică cunoașterea comunicării sau a datelor, permite interceptarea conținutului audio-video și a datelor schimbate sau permite interceptarea conversațiilor față în față; și colectează de la distanță pozițiile ocupate de echipamentele din teritoriu"); instrument/implant de investigație pe dispozitiv în Canada; dispozitiv tehnic în Țările de Jos (Regulamentul dispozitivelor tehnice în dreptul procesual penal publicat la 11 iulie 2018 și articolul 45 din Legea olandeză privind serviciile de securitate și informații); „software guvernamental" sau „GovWare" în Elveția (așa cum se indică în raportul explicativ al guvernului privind modificările aduse Codului penal elvețian).
[65] Disponibil aici; hotărârea nu este încă definitivă - cazul este pendinte la Curtea Supremă Federală.

colectarea informațiilor privind comunicațiile în direct și nici pentru datele de identificare ale acestora.[66] În **Germania**, câmpul de aplicare al „infiltrărilor tehnice/percheziţiilor online" (aşa cum sunt definite de Curtea Constituţională Federală) a fost considerabil limitat în urma unei hotărâri de referinţă a Curţii Constituţionale Federale (Decizia BvR 370/07).[67] În special, articolele 100d din Codul de procedură penală și articolul 49 § 7 din Legea Oficiului Federal de Poliție Criminală prevăd că, în cazul în care există elemente de fapt care să permită presupunerea că o măsură de căutare online va conduce doar la descoperiri în domeniul esențial al vieții private, măsura este inadmisibilă. În plus, pe cât posibil, trebuie să se ia măsuri tehnice pentru a se asigura că datele referitoare la domeniul esențial al vieții private nu sunt colectate. În urma Legii din iulie 2021 care urmărea adaptarea legii de protecție constituțională (Gesetz zur Anpassung des Verfassungschutzrechts), cele 19 servicii de informații germane au dreptul de a utiliza troieni pentru a citi comunicarea în curs pe calculatoare sau smartphone-uri și chiar date de comunicare din trecut.[68] În **Italia**, deși programul de supraveghere intruzivă are un potențial mare de intruziune,[69] Parlamentul italian a reglementat în mod expres utilizarea acestui instrument de anchetă numai pentru interceptarea conversațiilor față în față și numai pe dispozitive mobile. În **Luxemburg**, poliția poate utiliza programe spion pentru a captura date informatice, pe când Serviciile de Securitate pot căuta, într-o manieră țintită, informațiile necesare pentru îndeplinirea uneia dintre misiunile sale, sau monitorizarea și controlul comunicațiilor care nu pot fi interceptate din punct de vedere tehnic utilizând rețele normale de telecomunicații.[70] În **Țările de Jos**, legea nu definește datele care pot fi colectate de autoritățile de aplicare a legii, ci se referă mai degrabă la metodele prin care datele pot fi colectate sau modificate.[71] Serviciul General de Informaţii şi Securitate şi Serviciul Militar de Informaţii şi Securitate sunt autorizate să intercepteze, să primească, să înregistreze şi să asculte orice formă de conversaţie, telecomunicaţie sau transmitere a datelor utilizând un instrument tehnic printr-un lucru automatizat, indiferent de locația acesteia. Această autoritate include, de asemenea, puterea de a decripta conversațiile, telecomunicațiile sau transmisiile de date.[72] În **Norvegia**, citirea poate include comunicații, date stocate electronic și alte informații despre utilizarea sistemului informatic sau a contului de utilizator.[73] În **Spania**, articolul 588

[66] Articolul 23 § 2 din Legea privind măsurile coercitive, articolul 23 § 2 din Legea poliției și articolul 32 § 2 din Legea privind informațiile militare.
[67] BVerfG, Hotărârea Primului Senat din 27 februarie 2008 - 1 BvR 370/07 -, (traducere engleză), paragrafele 166 și următoarele. Această autoritate este totuși limitată la supravegherea comunicațiilor și nu permite accesul la alte informații de pe hard disk sau cloud. Programul utilizat trebuie să se limiteze strict la supravegherea comunicațiilor.
[68] Studiul PEGA, citat mai sus, § 4.5.
[69] Instrumentul folosit este potențial capabil să intercepteze comunicațiile dintre computere și sisteme telematice (e-mailuri, mesaje WhatsApp, conversații Skype etc.), să activeze microfoane și/sau camere și GPS, să înregistreze tot ceea ce este tastat pe tastatură (așa-numita funcție de înregistrare a tastelor) și tot ceea ce apare pe ecran (așa-numita funcție de capturi de ecran). De asemenea, se poate infiltra în memoria dispozitivelor în care sunt stocate datele, capturând astfel toate datele și informațiile conținute sau care trec prin dispozitivul infectat, precum și modificând orice informație stocată sau transmisă.
[70] Articolul 8 alineatul 1 litera (c) din Legea SRE.
[71] Aceste metode includ: (i) determinarea caracteristicilor lucrării automate sau ale utilizatorului, cum ar fi identitatea sau locația; (ii) executarea puterii speciale de investigare a interceptării țintite. Este posibil să interceptați comunicații, cum ar fi e-mailul sau cuvântul vorbit, folosind un dispozitiv tehnic (inclusiv software). Acest lucru este detaliat în raportul explicativ al Legii privind criminalitatea informatică III (de exemplu, seria parlamentară II 2015-2016, 34372, nr. 3, p. 9); (iii) executarea puterii speciale de investigare a observării sistematice, de exemplu, pentru a determina locația dispozitivului utilizat (de exemplu, seria parlamentară II 2015-2016, 34372, nr. 3, p. 14); (iv) înregistrarea datelor stocate în lucrarea automatizată; (v) inaccesibilizarea datelor, cum ar fi materialele care conțin abuzuri asupra copiilor (seria parlamentară II 2015-2016, 34372, nr. 3, p. 29), cfr. Articolul 126nba alineatul (1) litera (a) din Codul de procedură penală olandez.
[72] Articolul 47 alineatul (1) și articolul 45 alineatul (2) litera (b) litera (d) din Legea privind serviciile de securitate și de informații
[73] Articolul 216 o § 4. De remarcat este prevederea conform căreia citirea datelor trebuie aranjată astfel încât nicio informație să nu fie capturată în mod inutil despre utilizarea sistemului informatic de către altcineva decât suspectul. Citirea trebuie efectuată astfel încât să nu existe riscul inutil de întrerupere a funcționării sau de deteriorare a echipamentelor sau a datelor. Poliția trebuie să prevină, în măsura posibilului, riscul ca, ca urmare a punerii în aplicare, o persoană să poată obține acces neautorizat la sistemul informatic sau la informațiile protejate sau să comită alte infracțiuni.

septies(a) din Codul de procedură penală prevede că un program spion poate fi instalat pentru a examina conținutul unui calculator, dispozitiv electronic, sistem informatic, instrument de stocare a datelor în masă sau bază de date, fără cunoștința proprietarului sau a utilizatorului. În **Suedia**, programele spion pot fi folosite nu numai pentru a intercepta date sau pentru a monitoriza informațiile de comunicare și localizare, ci și pentru a efectua supravegherea audio și prin cameră.[74] În **Elveția**, utilizarea programelor spion în cadrul procedurilor penale este limitată fără echivoc la interceptarea și recuperarea conținutului comunicațiilor și metadatelor de telecomunicații în formă non-codată.[75] Nu există limitări aparente în ceea ce privește datele colectate în cadrul procedurilor de informații; cu toate acestea, articolul 26 § d din Legea Federală Elvețiană din 25 septembrie 2015 privind Serviciul de Informații („IntelSA") prevede că intruziunea în sistemele și rețelele informatice poate fi efectuată nu numai pentru a colecta informații disponibile acolo sau transmise de acolo, ci și pentru a perturba, împiedica sau încetini accesul la informații în cazul în care sistemele și rețelele informatice sunt utilizate pentru atacuri asupra infrastructurilor critice. În **Regatul Unit**, articolul 99 § 2 din Legea privind puterile de investigare din 2016 prevede că comunicațiile, datele despre echipamente sau orice alte informații care pot fi obținute printr-un mandat de interferență țintită a echipamentului.

42. În mai multe țări care utilizează programe spion, datele protejate de secretul profesional al unui avocat sau medic sau de secretul surselor unui jurnalist nu pot fi colectate sau analizate, sau există proceduri specifice[76].

C. Norme specifice *ratione materiae, personae* și *temporis* în statele care reglementează utilizarea programelor spion

[74] Cfr. Secțiunea 2 din Legea (2020:62) privind citirea datelor secrete. Statisticile publicate de procurorul general arată însă că autorizația de a activa supravegherea video de la distanță pe un dispozitiv a fost acordată doar de patru ori în 2023. Autorizația de a activa supravegherea audio de la distanță pe un dispozitiv a fost, de asemenea, acordată doar de patru ori în 2023.
[75] Articolul 269ter din Codul de procedură penală.
[76] A se vedea, de exemplu, în Belgia, articolul 18/9 § 4 din L. R&S prevede că o metodă excepțională poate fi utilizată împotriva unui avocat, medic sau jurnalist sau a mijloacelor de comunicare pe care le utilizează în scopuri profesionale, numai dacă serviciul de informații și securitate are dovezi prealabile serioase că avocatul, medicul sau jurnalistul este sau a fost implicat personal și activ în crearea sau dezvoltarea unei amenințări potențiale grave. Articolul 2 § 2 din lege interzice însă serviciilor de informații și securitate să obțină, să analizeze sau să exploateze date protejate de secretul profesional al unui avocat sau medic sau de secretul surselor unui jurnalist; în Finlanda, articolul 82 din Legea privind informațiile militare prevede că interceptarea telecomunicațiilor, colectarea de date, cu excepția interceptării telecomunicațiilor, interceptarea la fața locului, observarea tehnică, informațiile privind semnalele radio sau informațiile privind traficul de rețea nu vizează comunicațiile sau informațiile cu privire la care o parte nu poate depune mărturie sau are dreptul de a refuza să depună mărturie (secretul profesional în relația dintre un avocat și clientul său; privilegiul clerului și privilegiul medic-client). Dispoziții similare pot fi găsite în Legea privind măsurile coercitive și Legea poliției. În Luxemburg, articolul 88-2 § 6 alineatul (3) prevede că instalarea dispozitivului tehnic menționat la alineatele (2) și (3) ale articolului 88-1 nu poate fi efectuată, sub sancțiunea nulității, în spațiile utilizate în scopuri profesionale, în locuință sau în dependințele acesteia în sensul articolelor 479, 480 și 481 din Codul penal, sau vehiculul unui avocat, medic, jurnalist profesionist sau editor. În Țările de Jos, este prevăzută o procedură specială în cazul în care măsura de informații este efectuată împotriva unui jurnalist sau a unui avocat (art. 30 din Legea privind serviciile de informații și securitate din 2017). În cazul în care măsura de supraveghere este utilizată împotriva unui jurnalist și acest lucru poate duce la dezvăluirea identității unei surse a jurnalistului către serviciul de informații și securitate, autorizația pentru exercitarea acestei competențe trebuie acordată de instanța districtuală din Haga, mai degrabă decât de ministru. Instanța va aplica aceleași criterii pe care le-ar aplica altfel ministrul, inclusiv respectarea principiilor necesității, proporționalității și subsidiarității. Instanța poate autoriza exercitarea competenței pentru o perioadă de cel mult patru săptămâni, în loc de limita obișnuită de trei luni. În Suedia, Legea 2020:62 privind citirea datelor secrete (§ 11) interzice utilizarea supravegherii țintite prin intermediul programelor spion pe computerele sau telefoanele jurnaliștilor, avocaților, medicilor sau preoților; în Elveția, articolul 271 din Codul de procedură penală prevede că, în cazul supravegherii unei persoane care aparține uneia dintre categoriile profesionale enumerate la articolele 170-173, sortarea informațiilor care nu sunt relevante pentru obiectul anchetei sau pentru motivul pentru care persoana în cauză este supusă supravegherii trebuie efectuată sub conducerea unei instanțe. Această sortare se realizează în așa fel încât autoritățile de urmărire penală să nu fie la curent cu niciun secret profesional. Datele aruncate trebuie distruse imediat; nu pot fi utilizate. Sortarea preliminară a informațiilor menționate la alineatul (1) nu trebuie efectuată dacă: a. există motive serioase de suspiciune împotriva titularului secretului profesional și b. există motive speciale pentru a face acest lucru. Dispoziții similare sunt cuprinse la articolul 58 din Legea federală elvețiană din 25 septembrie 2015 privind serviciul de informații („IntelSA") pentru supravegherea țintită efectuată de serviciile de securitate.

43. După cum s-a menționat mai sus, anumite state au elaborat norme specifice pentru utilizarea instrumentelor de supraveghere intruzivă, cum ar fi programele spion, și au adaptat în consecință cerințele pentru ca agențiile de aplicare a legii și agențiile de informații să utilizeze aceste instrumente, în special în ceea ce privește aplicabilitatea *ratione materiae* și *temporis* a măsurii de supraveghere. Această secţiune oferă o imagine de ansamblu a acestor reguli specifice în statele care au raportat utilizarea de programelor spion.

1. *Ratione materiae*

44. În **Danemarca**, ancheta ar trebui să se refere la o infracțiune pedepsită prin lege cu închisoare de șase ani sau mai mult sau la o încălcare intenționată a capitolului 12 sau 13 din Codul penal.[77]

45. În **Germania**, se aplică lista mai restrânsă a infracțiunilor prevăzută la articolul 100b din Codul de procedură penală (mai degrabă decât cea prevăzută la articolul 100a). În cadrul anchetelor de informații, Oficiul Federal de Poliție Criminală poate accesa sistemele informatice numai dacă anumite fapte justifică presupunerea că există un pericol pentru (i) corpul, viața sau libertatea unei persoane sau (ii) bunurile publice, a căror amenințare afectează fundamentele sau existența federației sau a unei țări sau fundamentele existenței umane.[78]

46. În **Italia**, programele spion în cadrul procedurilor penale pot fi utilizate numai în cadrul unor infracțiuni deosebit de grave (cum ar fi, de exemplu, asociațiile criminale de tip mafiot)[79] sau, cu condiţia ca locurile şi orele în legătură cu care programele spion pot fi activate să fie determinate, chiar și indirect, și pentru infracțiuni comise de funcționari împotriva administrației publice pentru care se prevede o pedeapsă maximă cu închisoarea de cel puțin cinci ani.[80]

47. În **Luxemburg**, programele spion pot fi utilizate în cadrul procedurilor penale numai în cazul infracțiunilor grave, inclusiv infracțiuni împotriva securității statului[81] şi a actelor de terorism şi finanţare a terorismului;[82] în cadrul anchetelor de informaţii programele spion pot fi utilizate numai în prezenţa unei ameninţări sau a unui risc de ameninţare la adresa securităţii naţionale.[83]

48. În **Țările de Jos**, legiuitorul a prevăzut diferite exigențe în ceea ce privește gradul de intruziune al măsurii solicitate, în ceea ce privește gravitatea infracțiunilor. Pentru

[77] Secțiunea 791 (b) din Legea privind administrarea justiției.
[78] Articolul 49 § 1 din Legea Oficiului Federal de Poliție Criminală.
[79] Articolul 51 § 3-bis și 3-quater din Codul de procedură penală.
[80] În prima fază de aplicare, programul spion a fost introdus doar cu referire la cele mai grave infracțiuni de criminalitate organizată și terorism; extinderea în 2019 la infracțiunile împotriva administrației publice a făcut obiectul unor critici diferite, în ceea ce privește principiul proporționalității necesare, a se vedea *Senato della Repubblica, Documento approvato dalla 2ª Commissione permanente (Giustizia) nella seduta del 20 settembre 2023 a conclusione dell'indagine conoscitiva sul tema delle intercettazioni*, citată mai sus, p. 43.
[81] Astfel cum se prevede la articolele 101-123 din Codul penal.
[82] Astfel cum se prevede la articolele 135-1-135-6, 135-9 și 135-11-135-16 din Codul penal.
[83] Legea specifică în secțiunea 8 § 1 (c) natura potențialelor amenințări la adresa securității naționale: (i) spionaj și interferență; (ii) extremismul violent; (iii) terorism; (iv) proliferarea armelor de distrugere în masă sau a produselor și tehnologiilor legate de apărare; (v) criminalitatea organizată și amenințările cibernetice, în măsura în care acestea sunt legate de oricare dintre amenințările menționate mai sus. Legea exclude în mod explicit supravegherea politică internă din sfera de competență a serviciului de securitate. Domeniul de aplicare al acestei misiuni se extinde și la securitatea statelor străine și a organizațiilor internaționale și supranaționale cu care Luxemburgul a semnat acorduri.

trei categorii de metode prin care datele pot fi colectate sau modificate,[84] măsura poate fi solicitată în caz de bănuială a unei infracțiuni grave pentru care este permisă arestarea preventivă (în principal infracțiuni pentru care se prevede o pedeapsă de cel puțin patru ani). Alte două metode mai intruzive pot fi utilizate[85] doar pentru infracțiunile pentru care se prevede o pedeapsă de cel puțin opt ani sau stabilite ca infracțiune conform legii în decretul privind anchetele într-un sistem Informatic[86] sunt luate în considerare. Serviciile de informații pot utiliza programe spion atunci când țintele (persoane fizice sau organizații) reprezintă o amenințare la adresa securității naționale sau a ordinii democratice a Țărilor de Jos.[87]

49. În **Norvegia**, posibilitatea utilizării programelor spion este limitată la infracțiuni foarte grave, adică infracțiuni pentru care este prevăzută o pedeapsă de peste 10 ani de închisoare.[88]

50. În **Spania**, acest tip de măsură este autorizat numai pentru infracțiuni specifice (infracțiuni comise de organizații criminale, terorism, infracțiuni împotriva minorilor sau a persoanelor cu dizabilități, infracțiuni împotriva constituției, trădarea sau încălcarea apărării naționale, infracțiuni comise prin instrumente informatice).[89]

51. În **Suedia**, există o distincție între citirea datelor care nu implică și activarea microfonului unui dispozitiv pentru înregistrarea sunetului și cea care implică activarea microfonului unui aparat pentru a înregistra sunetul. În primul caz, se aplică o listă destul de largă a infracțiunilor pentru care este permisă interceptarea comunicațiilor.[90] Pentru citirea datelor secrete care implică activarea microfonului dispozitivului pentru înregistrarea sunetului, lista infracțiunilor permise este mult mai scurtă: numai cele pentru care se prevede o pedeapsă minimă de patru ani de închisoare, precum și un număr mic de infracțiuni legate securitate (spionaj etc.) pasibile de pedeapsă minimă mai redusă.[91]

52. În **Elveţia**, programele spion pot fi utilizate în cadrul procedurilor penale numai pentru lista restrânsă a infracțiunilor legate de anchete secrete, conform articolului 286 alin.(2) din CPP (pentru alte măsuri de supraveghere țintită, lista mai largă a articolului 269 se aplică). În anchetele de informații, articolul 27 din Legea privind informațiile limitează posibilitatea de a colecta informații la cazurile specifice menționate la articolul 19 § 2 punctele a) și d) sau la protecția altor interese naționale importante.

[84] În conformitate cu § 126nba § 1 (a): (i) identificarea și înregistrarea anumitor caracteristici ale sistemului informatic sau ale persoanei care îl utilizează, cum ar fi identitatea și locația sistemului informatic; (ii) ordinea de înregistrare a comunicațiilor după penetrare; (iii) Ordin de supraveghere sistematică.
[85] (iv) captarea datelor stocate în sistemul informatic; și (v) datele pot fi făcute inaccesibile, inclusiv ștergerea lor (temporară).
[86] Disponibil aici.
[87] Articolul 8 alineatul (2) litera (a) și articolul 10 alineatul (2) litera (a) din Legea privind serviciile de informații și de securitate.
[88] articolul 216 o și p; sau alte infracțiuni de activități ilegale de informații împotriva secretelor de stat, divulgarea de secrete de stat, alte activități ilegale de informații, participarea la asociații violente, influențarea serviciilor de informații străine, incitarea și recrutarea pentru terorism, călătorii cu intenția de a răspândi terorismul, participarea și recrutarea pentru activități militare ilegale în străinătate, infracțiuni de privare de libertate; traficul de ființe umane, producerea și diseminarea de materiale care sexualizează copiii, ascunderea, spălarea banilor, încălcarea Legii privind controlul exportului de produse, tehnologii strategice etc. și anumite încălcări ale Legii imigrației.
[89] Articolul 588septies din Codul de procedură penală.
[90] A se vedea secțiunea 4 din Legea (2020:62) privind citirea datelor secrete. Secțiunea 4 din Legea (2020:62) privind citirea datelor secrete, care face trimitere la capitolul 27, secțiunea 18a, din Codul de procedură judiciară.
[91] A se vedea secțiunea 6 din Legea (2020:62) privind citirea datelor secrete. Articolul 6 din Legea (2020:62) privind citirea datelor secrete, care face trimitere la capitolul 27 secțiunea 2d din Codul de procedură judiciară.

53. În **Regatul Unit**, se poate emite un mandat de interferență tematică țintită doar: (i) în interesul securității naționale, (ii) în scopul prevenirii sau detectării infracțiunilor grave sau (iii) în interesul bunăstării economice a Regatului Unit, în măsura în care aceste interese sunt relevante și pentru interesele securității naționale.[92]

54. În cele din urmă, se remarcă faptul că un criteriu standard de minimă intruziune/respectare a proporționalității este prezent în majoritatea statelor în care au fost colectate informații. Acest criteriu impune autorității solicitante să demonstreze, printre altele, că nu au existat alte mijloace mai puțin intruzive pentru a obține informațiile solicitate, iar organul de autorizare consideră că comportamentul autorizat este proporțional cu ceea ce se urmărește.[93]

2. *Ratione personae*

55. **Denmarca**, [94] **Finlanda**, [95] **Italia**, **Țările de Jos**, **Norvegia,**[96] **Spania**[97] limitează posibilitatea de a utiliza programele spion numai la dispozitivele deținute de persoanele bănuite de comiterea infracțiunilor prevăzute de lege sau de cei care prezintă amenințări la adresa securității naționale sau o amenințare echivalentă, așa cum este stabilit în cadrul juridic intern relevant. În **Belgia**, [98] **Germania**, [99] **Suedia**,[100] **Elveția**,[101] și **Regatul Unit**, [102] terţii care sunt suficient de legați de ținta principală pot fi, de asemenea, obiectul unei supravegheri prin program spion.

3. *Ratione temporis*

56. Din analiza comparativă rezultă că termenele pentru autorizarea utilizării programelor spion ca instrument de supraveghere țintită sunt, în majoritatea cazurilor examinate, mai scurte atunci când se acordă autorizațiile în cadrul procedurilor penale în comparație cu autorizațiile din cadrul anchetelor de informații.

---

[92] Articolul 102 alineatul (5) din Legea din 2016 privind competențele de investigare.

[93] De exemplu, în Belgia (articolul 90ter § 1 din Codul de procedură penală); în Canada [secțiunea 21 § 2 (b) din Legea canadiană a Serviciului de Informații de Securitate); în Suedia [articolul 3 din Legea (2020:62) privind citirea datelor secrete]; în Elveția (articolul 27 din IntelSA); în Regatul Unit [articolul 102 alineatul (1) litera (b) din Legea din 2016 privind competențele de investigare].

[94] Secțiunea 791 (b) din Legea privind administrarea justiției.

[95] Articolul 23 § 3 din Legea privind măsurile coercitive.

[96] Articolul 216 o § 4 din Legea de procedură penală. În ceea ce privește investigațiile de informații, ar trebui clarificat faptul că serviciul de informații nu poate utiliza supravegherea specifică sau alte forme de supraveghere a persoanelor din Norvegia. O interdicție explicită este prevăzută la articolul 4 alineatul (1) din Legea din 2020 privind serviciile de informații.

[97] Articolul 588septies litera (c) din Codul de procedură penală.

[98] Articolul 90-ter § 1 din Codul de procedură penală: se poate dispune supravegherea persoanelor despre care se presupune, pe baza unor fapte specifice, că comunică în mod regulat cu un suspect.

[99] În conformitate cu articolul 100b alineatul 3 din Codul de procedură penală, în cazul în care există motive să presupunem, pe baza anumitor fapte, că: (i) inculpatul utilizează sistemele informatice ale celeilalte persoane; și (ii) interferența cu sistemele de tehnologie a informației ale acuzatului nu va stabili faptele sau nu va determina locul în care se află un co-acuzat. A se vedea, de asemenea, articolul 49 § 3 din Legea Oficiului Federal de Poliție Criminală (în cazul în care este inevitabil).

[100] Secțiunea 4a din Legea (2020:62) privind citirea datelor secrete.

[101] În cadrul procedurilor penale, articolul 270 din Codul de procedură penală prevede că, pe lângă acuzat, terții pot fi monitorizați dacă există informații specifice că: (i) inculpatul utilizează adresa poștală sau serviciul de telecomunicații al terțului sau (ii) terțul primește anumite comunicări în numele acuzatului sau transmite comunicări de la inculpat către o altă persoană. În mod similar, Serviciul Federal de Informații poate dispune o măsură de căutare a informațiilor pe bază de autorizare împotriva unui terț în cazul în care există motive să se creadă că persoana de la care se intenționează colectarea de informații utilizează spații, vehicule sau depozite care aparțin terțului sau adrese poștale; puncte de conectare la telecomunicații, sisteme informatice sau rețele informatice ale acestora din urmă pentru a transmite, primi sau stoca informații [articolul 28 din Legea federală din 25 septembrie 2015 privind Serviciul de Informații („LSCR")]. Măsura nu poate fi dispusă dacă terțul aparține unuia dintre grupurile profesionale menționate la articolele 171-173 din Codul de procedură penală.

[102] Secțiunea 101 al IPA 2016.

57. În cadrul procedurilor penale, în statele care utilizează programele spion, termenele variază de la 15 zile[103] la șase luni,[104] sau pe perioade raportate de la 4 săptămâini,[105] o lună[106] sau trei luni.[107]

58. În anchetele de informații, acest lucru durează de la patru săptămâni,[108] la șase luni,[109], alte țări prevăd termene de o lună,[110] 40 zile,[111] două luni,[112] sau trei luni.[113]

D. Autorizarea măsurilor de supraveghere țintită

59. În măsura în care autorizarea măsurilor de supraveghere țintită în cadrul anchetelor/procedurilor penale este încredințată sistemului judiciar în majoritatea covârșitoare a statelor în care sunt disponibile date,[114] abordarea diferă în ceea ce privește autorizarea măsurilor de supraveghere țintită în cadrul anchetelor de informații. În **Franța**,[115] **Germania**,[116] **Luxemburg**,[117] **Țările de Jos**,[118] o astfel de autorizație este încredințată executivului, susținută de un organ independent de autorizare. În **Belgia**, este necesară o decizie motivată a șefului departamentului de servicii de securitate, în urma aprobării unei comisii administrative specializate.[119] În

[103] Italia (articolul 267 alineatul 3 din Codul de procedură penală), Norvegia (articolul 216 alineatul 5 din Codul de procedură penală).
[104] Regatul Unit, articolul 116 § 2 litera (b) din Legea privind competențele de investigare).
[105] Danemarca (articolul 783 din Legea privind administrarea justiției), Țările de Jos (articolul 126nba § 3 din Codul de procedură penală).
[106] Belgia (articolul 90quater din Codul de procedură penală); Finlanda (articolul 24 din Legea privind măsurile coercitive); Germania (articolul 100e alineatul 2 din Codul de procedură penală - după o perioadă totală de șase luni, instanța regională superioară decide cu privire la orice ordin de prelungire ulterioară); Luxemburg (articolul 88-2 § 4 - reînnoit pentru o perioadă totală maximă de un an); Spania [articolul 588septies (c) din Codul de procedură penală - reînnoit pentru o perioadă totală maximă de trei luni); Suedia [articolul 18 din Legea (2020:62) privind citirea datelor secrete - reînnoibilă; legea prevede, de asemenea, că, în cazul în care condițiile autorizației s-au schimbat, supravegherea trebuie să înceteze imediat. Cifrele pentru 2023 arată că perioada medie de autorizare a fost de 21 de zile, perioada mediană fiind de 13 zile.
[107] Elveția (articolul 274 din Codul de procedură penală).
[108] Danemarca (articolul 783 din Legea privind administrarea justiției))
[109] Finlanda (articolul 24 din Legea poliției și articolul 33 din Legea privind informațiile militare); Regatul Unit [articolul 116 § 2 litera (b) din Legea privind competențele de investigare].
[110] Suedia [articolul 18 din Legea (2020:62) privind citirea datelor secrete - reînnoibilă; legea prevede, de asemenea, că, în cazul în care condițiile autorizației s-au schimbat, supravegherea trebuie să înceteze imediat. Cifrele pentru 2023 arată că perioada medie de autorizare a fost de 21 de zile, perioada mediană fiind de 13 zile.
[111] Italia (articolul 4-bis § 1 din Legea nr. 144/2005)
[112] Belgia (articolul 18/10 § 1).
[113] Germania (articolul 49 § 6 alineatul (3) din Legea privind Oficiul Federal de Poliție Criminală); Luxemburg (articolul 7 alineatul 1 din Legea SRE), Țările de Jos (articolul 49 alineatul 4 din Legea privind serviciile de informații și de securitate din 2017), Spania (articol unic, Legea 2/2002 care reglementează controlul jurisdicțional prealabil al Centrului Național de Informații); Elveția (articolul 26 § 6 din IntelSA).
[114] Excepții notabile sunt Irlanda, Malta și Regatul Unit, a se vedea notele de subsol 120, 146 și, respectiv, 121 de mai jos.
[115] În cazul în care prim-ministrul decide să nu ia în considerare un aviz negativ emis de Comisia Națională pentru Controlul Tehnicilor de Informații (CNCTR), CNCTR trebuie să sesizeze imediat Consiliul de Stat. Consiliul ia decizia finală.
[116] În Germania, serviciile federale de informații nu au voie să intercepteze telecomunicațiile la sursă până când nu au primit un ordin de la Ministerul Federal al Afacerilor Interne și al Comunității și operațiunea nu a fost autorizată de Comisia G10 (o comisie compusă din cinci membri, dintre care cel puțin trei trebuie să fie împuterniciți să exercite funcții judiciare, numit de grupul de control parlamentar), în timp ce Serviciul Federal de Informații (BND) trebuie să obțină autorizația Consiliului Independent de Control (Unabhängiger Kontrollrat) înainte de a putea lua măsuri pentru a opera rețelele informatice. În conformitate cu articolul 23 alineatul 7 din Legea privind Serviciul Federal de Informații, Consiliul trebuie să autorizeze căutarea datelor înainte ca acestea să fie utilizate. În caz de urgență, un membru al Consiliului poate autoriza astfel de măsuri, dar acestea trebuie să fie examinate de Consiliu cât mai curând posibil.
[117] Ordonat de Comitetul ministerial de informații la cererea scrisă a directorului Agenției Naționale de Informații și după aprobarea unei comisii speciale formate din judecători de rang înalt, și anume președintele Curții Superioare de Justiție, președintele Curții Administrative și președintele Tribunalului Districtual din Luxemburg [articolul 7 alineatul (4) din Legea SRE].
[118] Șeful Serviciului General de Informații și Securitate (AIVD) sau al Serviciului Militar de Informații și Securitate (MIVD). Un ministru trebuie să autorizeze utilizarea acestei puteri de investigare în temeiul secțiunii 45 din Legea serviciilor de informații și securitate. Comisia pentru competențe de investigare (TIB) examinează în continuare legalitatea utilizării acestei puteri înainte de a fi utilizată.
[119] Comisia pentru controlul metodelor specifice și excepționale de colectare a datelor din cadrul serviciilor de informații și securitate (Comisia BIM), compusă din trei magistrați și prezidată de un judecător de instrucție.

Irlanda[120] și **Regatul Unit**,[121] atât executivul, cât și sistemul judiciar au de jucat un rol în procedura de autorizare a măsurilor de supraveghere țintită. În **Bulgaria**, **Bosnia și Herțegovina,** [122] **Canada**, **Croatia**, [123] **Danemarca**, **Estonia**, [124] **Finlanda**, [125] **Grecia**, [126] **Islanda**, **Italia,** [127] **Kosovo,** [128] **Kyrgyzstan, Lithuania,** [129] **Republica Moldova,** [130] **Monaco**, **Macedonia de Nord**, [131] **Norvegia**, [132] **Portugalia**, [133]

[120] Autorizația judiciară este necesară pentru anumite tipuri de dispozitive de supraveghere (cum ar fi instalarea de microfoane audio sau camere video secrete) în conformitate cu Legea privind justiția penală (supravegherea) din 2009, în timp ce autorizația executivului (ministrul justiției) este necesară pentru interceptarea comunicațiilor telefonice în conformitate cu Legea din 1993 privind interceptarea pachetelor poștale și a telecomunicațiilor. Legea privind comunicațiile (păstrarea datelor) din 2011, astfel cum a fost modificată prin Legea din 2022, conferă Înaltei Curți competența de a păstra Anexa 2 (Localizarea comunicațiilor și datele de trafic). Accesul la datele sursă de pe Internet și la datele din Anexa 2 este acordat de un judecător al Tribunalului Districtual. Când vine vorba de datele utilizatorilor, nu este necesar să obțineți permisiunea unui judecător sau a unui organism independent.

[121] Secțiunea 108 din Legea privind competențele de investigare: În investigațiile penale și de informații, Comisarul pentru competențe de investigare (IPC) aprobă mandate de interferență a echipamentelor la cererea autorităților publice, cum ar fi secretarul de stat, agențiile de informații, poliția și autoritățile locale. IPC este asistat de o echipă de comisari judiciari. Aceștia sunt numiți de prim-ministru și trebuie să dețină sau să fi deținut funcții judiciare înalte.

[122] Președintele Curții Bosniei și Herțegovinei sau un judecător delegat de acesta. O decizie a Curții Constituționale a Bosniei și Herțegovinei (U-21/16 din 1 iunie 2017) a declarat neconstituțională prevederea (articolul 78 alineatele (3, 4 și 5 din Legea privind Agenția de Informații și Securitate a Bosniei și Herțegovinei) care acorda anterior directorului general al Agenției pentru Servicii de Securitate posibilitatea de a aproba măsura de informații cu acordul președintelui Consiliului de Miniștri al Bosniei și Herțegovinei în cazul în care întârzierea a cauzat prejudicii ireparabil pentru securitatea Bosniei și Herțegovinei. Întemeindu-se pe jurisprudența Curții Europene a Drepturilor Omului, Curtea a statuat că legea nu impune directorului general să trimită o cerere scrisă judecătorului și nici nu precizează termenul în care judecătorul trebuie să aprobe sau să suspende aplicarea unor astfel de măsuri.

[123] Este necesar un mandat judiciar de la cea mai înaltă instanță (Curtea Supremă a Republicii Croația) pentru următoarele măsuri mai intruzive: supravegherea sub acoperire a conținutului comunicațiilor, cenzura poștală (supravegherea sub acoperire a corespondenței și a altor corespondențe), supravegherea sub acoperire și înregistrarea tehnică a interiorului instalațiilor, spațiilor închise și obiectelor, precum și supravegherea și controlul sub acoperire, cu înregistrarea audio a conținutului comunicațiilor dintre persoane în spații deschise și publice (articolul 36 din Legea privind sistemul de securitate și informații din 2006). Alte măsuri mai puțin intruzive, cum ar fi supravegherea sub acoperire a datelor de trafic din telecomunicații, localizarea utilizatorilor și telecomunicațiile internaționale, supravegherea și controlul sub acoperire, cu înregistrarea imaginilor și fotografiilor persoanelor în spații deschise și publice, achiziționarea secretă de documente și obiecte, pot fi luate dacă sunt aprobate de unul dintre directorii agențiilor de securitate și informații din în domeniile lor de activitate respective (articolul 38).

[124] Președintele unei instanțe administrative sau un judecător administrativ numit de acesta.

[125] Dar simpla instalare și îndepărtare a unui dispozitiv sau a unui software nu necesită autorizarea unei instanțe, a se vedea articolul 42 din Legea privind informațiile militare și articolul 26 din Legea privind măsurile coercitive.

[126] În conformitate cu articolul 4 din Legea 5002/2022, ordinul relevant (διάταξη) este emis de procurorul competent în urma unei cereri din partea Agenției Naționale de Informații a Greciei (EYP). Cu toate acestea, procurorul competent este detașat (αποσπασμένος) pentru o repartizare cu normă întreagă la EYP (în conformitate cu articolul 5 alineatul 3 din Legea 3649/2008) și, prin urmare, independența sa este adesea contestată. Ordinul procurorului PEJ trebuie confirmat de un al doilea procuror (de rang înalt) care servește fie la Curtea de Apel, fie la Curtea Supremă (Areios Pagos).

[127] Articolul 4 din Decretul-lege nr. 144 din 27 iulie 2005 conferă Președintelui Consiliului de Miniștri competența de a autoriza directorii serviciilor de informații de securitate menționate la articolul 2 alineatul (2) din Legea nr. 124 din 3 august 2007 să solicite autorizarea interceptării comunicațiilor sau conversațiilor, inclusiv prin mijloace telematice, și să intercepteze comunicații sau conversații, chiar și în locurile menționate la articolul 614 din Codul penal. 124 din 3 august 2007 să solicite autorizația de a intercepta comunicații sau conversații, inclusiv prin mijloace telematice, precum și de a intercepta comunicații sau conversații, chiar și în locurile prevăzute la articolul 614 din Codul penal, dacă acest lucru este considerat necesar pentru îndeplinirea sarcinilor care le sunt încredințate prin articolele 6 și 7 din Legea nr. 124 din 3 august 2007. Autorizația se solicită de la Parchetul de pe lângă Curtea de Apel din Roma, care o acordă dacă sunt îndeplinite condițiile prevăzute la articolul 4-bis.

[128] Un judecător al Curții Supreme la cererea directorului sau directorului adjunct al Agenției de Informații din Kosovo (KIA), a se vedea Legea nr. 03/L-063 privind Agenția de Informații din Kosovo.

[129] Articolul 10 din Legea privind obținerea de informații criminale.

[130] Cu condiția ca percheziția obiectelor și documentelor, supravegherea vizuală și colectarea de informații să poată fi dispuse cu autorizarea șefului subdiviziunii specializate a serviciilor de securitate, cf. Articolul 27 coroborat cu articolul 20 din Legea nr. 59/2012 privind activitatea specială de investigare.

[131] Un judecător al Curții Supreme la cererea procurorului general al Republicii Macedonia de Nord, la inițiativa ministrului de interne sau a ministrului apărării (articolul 20 din Legea privind supravegherea comunicațiilor).

[132] Deciziile privind colectarea de informații electronice transfrontaliere (traficul pe internet) trebuie aprobate de o instanță (a se vedea articolul 8-1 din Legea privind informațiile din 2020).

[133] Un complet format din trei judecători ai camerelor penale ale Curții Supreme de Justiție.

România, **Serbia**,[134] **Slovacia**,[135]**Spania**,[136] **Suedia**,[137]**Ucraina**,[138] **Statele Unite**[139] puterea de autorizare este încredințată sistemului judiciar. În **Coreea,** măsurile de supraveghere țintită în cadrul investigațiilor de informații necesită fie autorizația președintelui Înaltei Curți, fie aprobarea Președintelui Republicii**.** [140] În **Polonia** puterea de autorizare este în mod normal încredințată sistemului judiciar,[141] însă, în ceea ce privește supravegherea secretă a resortisanților străini, un regim special permite autorităților să efectueze o supraveghere secretă timp de trei luni fără o autorizație judiciară prealabilă.[142] În **Elveția** situația este diferită în funcție de faptul dacă ținta este în Elveția sau în străinătate. În primul caz, sunt implicate atât sistemul judiciar, cât și executivul.[143] În al doilea caz, nu este necesară nicio autorizație judiciară.[144] În **Ungaria** [145] și **Malta** [146] competența de a autoriza măsuri de supraveghere țintită în cadrul anchetelor privind informațiile este încredințată executivului.

60. În multe state există posibilitatea ca agențiile de aplicare a legii sau serviciile de informații, în cazuri excepționale și urgente (de exemplu, un pericol pentru viața umană, sănătate, etc, securitatea publică sau a statului) să efectueze o supraveghere țintită în absența unei autorizații prealabile, cu condiția ca autorizația să fie acordată

[134] În conformitate cu Legea privind Agenția pentru Informații de Securitate (articolul 15), decizia la propunerea motivată a directorului Agenției este luată de președintele Înaltei Curți din Belgrad, adică de un judecător pe care îl deleagă dintre judecătorii Departamentului special al acestei Curți, care, în conformitate cu legea, se ocupă de cauzele referitoare la infracțiuni legate de criminalitatea organizată, corupție și alte infracțiuni deosebit de grave.

[135] În conformitate cu articolul 4a din Legea privind protecția împotriva interceptării (PAIA), instanța competentă este instanța regională în a cărei circumscripție se află autoritatea publică solicitantă. Singura excepție este pentru infracțiunile care intră în competența Curții Penale Specializate.

[136] Consiliul General al Magistraturii numește un judecător al Curții Supreme (al camerei administrative sau penale) și un adjunct pentru a autoriza interceptarea comunicațiilor de către serviciile de informații. Ambii trebuie să aibă cel puțin trei ani de vechime la Curtea Supremă. Mandatul lor este de cinci ani. Acest judecător poate autoriza interceptarea comunicărilor la propunerea directorului CNI. La 8 septembrie 2023, grupul parlamentar al Partidului Naționalist Basc a prezentat un proiect de lege pentru modificarea Legii 11/2002 și a Legii organice 2/2002. Proiectul de lege propune consolidarea controlului judiciar prealabil prin înlocuirea figurii unui singur magistrat al Curții Supreme responsabil de aceste chestiuni cu o cameră de trei magistrați ai Curții Supreme. Proiectul de lege a fost adoptat ca inițiativă completă de către Congres pe 27 februarie 2024, dar nu a trecut încă de Senat.

[137] Articolul 14 din Legea (2020:62) privind citirea datelor secrete.

[138] Articolul 15 § 2 din Legea privind informațiile nr. 912-IX prevede că o agenție de informații poate începe să desfășoare activități de informații numai pe baza unei decizii judecătorești. Prin decizia șefului agenției de informații, o măsură de informații poate fi prelungită până la obținerea unei hotărâri judecătorești, dar nu mai mult de 72 de ore de la momentul identificării persoanei.

[139] O instanță specializată (Curtea de Supraveghere a Informațiilor Externe a Statelor Unite) servește ca organism de aprobare pentru utilizarea instrumentelor de supraveghere. Colectarea comunicațiilor electronice de la non-americani aflați în afara Statelor Unite nu necesită un mandat.

[140] Aprobarea prezidențială este necesară numai în circumstanțe speciale, în timp ce autorizarea judiciară este procedura normală.

[141] Cererea de control operațional se depune la instanța districtuală competentă (sąd okręgowy), împreună cu documentele care justifică necesitatea punerii sale în aplicare. Cererile de autorizare a supravegherii sunt examinate de judecători unici și, în conformitate cu articolul 47a din Legea privind sistemul judiciar comun (Ustawa o ustroju sądów powszechnych), sunt atribuite unui judecător de serviciu. La reuniune pot participa un procuror și un reprezentant al autorității care solicită controlul operațional.

[142] articolul 9 § 1 din Legea antiterorism; a se vedea Pietrzak și Bychawska-Siniarska și alții v. Polonia, citată mai sus, §§ 53-54.

[143] Măsura de informații trebuie să fie autorizată de președintele unei secții speciale a Curții Administrative Federale (articolul 29 din IntelSA). În plus, măsura trebuie să fie autorizată de ministrul apărării după consultarea ministrului afacerilor externe și a ministrului justiției. Consiliul Federal trebuie să fie informat cu privire la cazurile de importanță deosebită (art. 30 IntelSA).

[144] Numai Consiliul Federal este împuternicit să decidă cu privire la atacurile împotriva rețelelor de calculatoare (articolul 37 § 1 din IntelSA). În cazul exploatării rețelelor de calculatoare (§ 2), ministrul apărării este ministrul apărării, după consultarea miniștrilor afacerilor externe și justiției.

[145] Conform Legii securității naționale, ministrul justiției este responsabil pentru acordarea acestei autorizații.

[146] În conformitate cu capitolul 391 din Legea privind serviciile de securitate, Serviciul de securitate din Malta poate obține permisiunea de a intercepta sau de a interfera cu comunicațiile prin intermediul unui mandat emis de ministrul responsabil cu Serviciul de securitate, care este, în general, ministrul afacerilor interne. Legea se aplică și procedurilor penale.

de organismul de autorizare relevant într-un termen care variază între 24 de ore[147], două zile [148], trei zile[149] și cinci zile.[150]

E. Mecanismele de control

61. Datele de care dispune Comisia de la Veneția arată că sistemele naționale de control sunt diverse în ceea ce privește cadrele juridice, organizarea, componența, mandatul, funcțiile și competențele acestora. O gamă largă de actori diferiți par să fie implicați în sistemele naționale de control, inclusiv în sistemul judiciar (curți sau tribunale sau organisme judiciare similare), parlamente (sub-)comisii parlamentare specializate), instituții naționale independente (de exemplu, ombudsmani) și agenții de control specializate (cu un mandat special de control) care nu fac parte din Parlament, din executiv sau din agențiile pe care le controlează.[151]

62. Controlul măsurilor de supraveghere țintită dispuse în cadrul procedurilor penale este, în mod normal, încredințată sistemului judiciar în cadrul controlului general a procedurii în curs.[152]

63. În ceea ce privește controlul măsurilor de monitorizare desfășurate de agențiile de informații, Comisia de la Veneția a observat că organele de experți independenți

[147] Croația (articolul 36 § 2 din Legea privind sistemul de securitate și informații al Republicii Croația); Danemarca (articolul 783 din Legea privind administrarea justiției); Estonia (articolul 1264 § 2 și § 3 din Codul de procedură penală); Finlanda (articolul 24 din Legea privind măsurile coercitive, articolul 24 din Legea privind poliția și articolul 33 din Legea privind informațiile militare); Republica Slovacă, secțiunea 114 § 2 din Legea privind administrarea justiției (PAIA)).

[148] Italia (articolul 267 din Codul de procedură penală); Kosovo (Legea nr. 03/L-063 privind Agenția de Informații din Kosovo), România (articolul 141 alineatul 1 din Codul de procedură penală), San Marino (articolul 4 din Legea nr. 98 din 21 iulie 2009 ("Legea privind interceptările"))

[149] Kosovo (în cadrul procedurilor penale - articolul 90 alineatul 2 din Codul de procedură penală); Ucraina (articolul 15 din Legea "informațiilor"); Regatul Unit [articolul 109 alineatul (3) din IPA 2016).

[150] Polonia, articolul 19 § 3 din Legea privind poliția.

[151] O prezentare generală a mecanismelor de control în vigoare în țările UE în contextul supravegherii informațiilor poate fi găsită în raportul FRA, citat mai sus. A se vedea, de asemenea, Consiliul Europei, Comisarul pentru drepturile omului, supravegherea democratică și eficace a serviciilor naționale de securitate, mai 2015.

[152] Există câteva excepții notabile: în Olanda, pe lângă supravegherea judiciară în timpul procesului, autoritatea de inspecție a Ministerului Justiției și Securității are un mandat special de a verifica (în principal procedurile) utilizarea hacking-ului informatic ca mijloc de investigare. Acesta prezintă un raport anual, dar nu are competențe obligatorii pentru a remedia situația. În Norvegia, articolul 216h din Legea de procedură penală din 1981 impune înființarea unui organism independent care să monitorizeze legalitatea utilizării și stocării măsurilor de control al comunicațiilor (interceptarea convorbirilor telefonice, supravegherea, interceptarea datelor). Acest organism, compus din cel puțin 3 membri (în prezent 6 membri), este numit de guvern. Președintele trebuie să îndeplinească cerințele pentru a fi judecător al Curții Supreme. Organismul se poate ocupa de orice problemă ridicată de persoane sau organizații cu privire la supravegherea poliției. De asemenea, organismul poate, din proprie inițiativă, să se ocupe de orice problemă și trebuie să acorde prioritate problemelor care au făcut obiectul dezbaterii publice sau al criticilor. Organismul are acces la toate informațiile referitoare la măsurile de control al comunicațiilor, inclusiv interceptarea telefonului, video, interceptarea datelor etc. În Suedia, pe lângă controlul judiciar, Comisia pentru securitate și protecția integrității (a se vedea Legea privind supravegherea anumitor activități de combatere a criminalității 2007:980) are mandatul de a se asigura că: activitățile de supraveghere a poliției, inclusiv poliția de securitate, și arhivarea datelor cu caracter personal de către aceasta din urmă, se desfășoară în conformitate cu legile și alte reglementări. Este un organism de 10 membri numiți de guvern pentru o perioadă de până la patru ani. Toate partidele reprezentate în Riksdag pot propune un membru al Comisiei. Majoritatea partidelor au numit politicieni cu experiență, dintre care unii sunt parlamentari activi. Președintele și vicepreședintele trebuie să fie sau să fi fost judecători titulari sau să aibă experiență juridică echivalentă. Articolul 2 din Legea privind supravegherea prevede că NAS își exercită supravegherea prin inspecții și alte investigații. În fiecare an, acesta preia o serie de cazuri din proprie inițiativă. SIN prezintă un raport anual guvernului. O prevedere importantă este că, spre deosebire de alte măsuri secrete de investigare, cum ar fi interceptarea telecomunicațiilor, în cazurile de citire a datelor secrete, instanța care eliberează autorizația are obligația de a informa NAS atunci când a fost acordată o autorizație (articolul 21 din Legea privind citirea secretă a datelor). Această obligație pro-activă permite SIN să aibă o imagine de ansamblu mai bună asupra modului în care este aplicată legea și să decidă dacă să deschidă sau nu o investigație de monitorizare. În Regatul Unit, Tribunalul Competențelor de Investigare (IPT) este un tribunal complet independent responsabil cu examinarea plângerilor privind abuzul de competențe de investigare. Este compusă din oameni care au deținut funcții judiciare înalte (iar președintele trebuie să fie o astfel de persoană) și avocați cu experiență. Tribunalul are, de asemenea, competența de a acorda despăgubiri și poate dispune distrugerea informațiilor și a dosarelor de informații, precum și anularea mandatelor.

efectuează acest control în mai multe țări, în special în **Austria**,[153] **Belgia**,[154] **Bulgaria**,[155] **Canada**,[156] **Croația**,[157] **Danemarca**,[158] **Finlanda**,[159] **Franța**,[160] **Germania**,[161] **Grecia**,[162] **Lituania**,[163] **Țările de Jos**,[164] **Macedonia de Nord**,[165]

[153] Responsabilul cu protecția juridică este responsabil de supravegherea prelucrării datelor menționate la articolul 12 alineatele (1) și (1a) din Legea privind securitatea și informațiile de stat, precum și de protecția juridică menționată la articolul 6 alineatele (1) și (2) din lege. Unitățile organizaționale competente trebuie să obțină autorizația prealabilă înainte de a îndeplini sarcinile menționate la articolul 6 alineatele (1) și (2) din lege. Acesta trebuie să aibă acces la toate documentele, evidențele și datele prelucrate necesare, precum și la toate spațiile în condițiile prevăzute de lege. De asemenea, poate depune o plângere la autoritatea de protecție a datelor în numele persoanelor vizate. În fiecare an, ofițerul de protecție juridică raportează ministrului de interne cu privire la activitățile și percepțiile sale în îndeplinirea atribuțiilor sale [articolul 15 alineatul (4) din lege]. De asemenea, Direcția raportează ministrului de interne și publică un raport anual privind evoluțiile actuale și posibile în protecția constituției pentru a informa publicul. Comisia Independentă de Audit pentru Protecția Constituției este responsabilă de monitorizarea activităților unităților organizaționale și de investigarea acuzațiilor privind activitățile unităților organizaționale. Comisia are acces la toate spațiile și poate inspecta documentele și evidențele. Acesta prezintă un raport anual ministrului federal de interne și Subcomisiei permanente a Comisiei pentru afaceri interne (a Consiliului Național) și întocmește un raport anual de informare a publicului cu privire la activitățile sale. Acesta poate face în orice moment recomandări ministrului federal de interne.

[154] Comitetul permanent R este responsabil de supravegherea funcționării generale a serviciilor de informații și de securitate. Este un organism colegial: este compus din trei membri, inclusiv un președinte care trebuie să fie magistrat. Acesta controlează legalitatea deciziilor privind metode specifice și excepționale, precum și respectarea principiilor proporționalității și subsidiarității. În cazul în care Comitetul permanent R constată că o metodă este ilegală sau că principiul proporționalității sau subsidiarității nu a fost respectat, acesta poate pune capăt metodei. Toate informațiile colectate folosind această metodă trebuie apoi distruse.

[155] Oficiul Național pentru Controlul Resurselor Speciale de Informații.

[156] Agenția Națională de Securitate și Informații (NSRA) este un organism de supraveghere independent și extern care raportează Parlamentului. NSIRA are autoritatea de a revizui activitățile de securitate națională și de informații ale guvernului Canadei pentru a se asigura că acestea sunt legale, rezonabile și necesare. În urma unei revizuiri, NASS poate face orice concluzii sau recomandări pe care le consideră adecvate. NSIRA investighează, de asemenea, plângerile publice cu privire la agențiile și activitățile cheie de securitate națională, precum și plângerile privind autorizațiile de securitate. În urma unei investigații, NSIRA trebuie să furnizeze un raport care să conțină concluziile investigației și orice recomandări pe care le consideră adecvate. Concluziile și recomandările făcute de NSIRA nu sunt obligatorii.

[157] Consiliul pentru Controlul Civic al Agențiilor de Informații de Securitate efectuează monitorizarea periodică a agențiilor, concentrându-se pe legalitatea activității și implementarea măsurilor speciale de colectare a datelor. Acesta acționează pe baza solicitărilor transmise de cetățeni și persoane juridice cu privire la potențiale nereguli și încălcări ale drepturilor omului. Consiliul este alcătuit din șapte cetățeni numiți de Parlament pe baza unui apel public pentru mandate de patru ani, dar cu expertiză specifică și autorizație de securitate completă. În cazul în care, în cursul inspecției efectuate, se constată că au avut loc acte ilegale, Președintele Consiliului informează Președintele Republicii, Președintele Parlamentului, Președintele Guvernului și Procurorul General al Statului.

[158] Consiliul danez de supraveghere a serviciilor de informații are puterea de a accesa toate datele colectate de serviciile de securitate.

[159] Ombudsmanul pentru informații supraveghează autoritățile de informații civile și militare: Serviciul finlandez de informații și securitate, Divizia de informații a Comandamentului apărării și Agenția finlandeză de informații a apărării. În conformitate cu articolul 15 din Legea privind controlul colectării de informații, Ombudsmanul pentru informații este împuternicit să dispună suspendarea sau încetarea utilizării metodei de informații în cazul în care consideră că autoritatea de informații a acționat în mod ilegal în colectarea de informații.

[160] CNCTR se asigură că colectarea informațiilor se realizează în conformitate cu Codul de securitate internă. Potrivit articolului L831-1 din Cod, CNCTR este compusă din patru parlamentari (doi deputați și doi senatori), doi membri ai Consiliului de Stat, doi magistrați și un expert în tehnici de comunicare electronică. Comisia poate emite avize cu privire la punerea în aplicare a tehnicilor de colectare a informațiilor, dar acestea nu sunt obligatorii.

[161] Comisia G10 și Consiliul independent de supraveghere. Prima este constituită de Parlament în conformitate cu articolul 10 § 2 din Grundgesetz german și se limitează la măsurile privind telecomunicațiile. Acesta înlocuiește controlul exercitat de sistemul judiciar. Al doilea acționează ca un organism de control administrativ. Membrii săi sunt șase judecători ai Curții Supreme Federale și/sau ai Curții Administrative Federale, care sunt aleși de grupul de control parlamentar pentru 12 ani.

[162] Autoritatea Elenă pentru Securitatea Comunicațiilor și Protecția Confidențialității (ADAE). În conformitate cu articolul 6 din Legea nr. 3115/2003, ADAE este autorizată să efectueze audituri ale instalațiilor, echipamentelor, arhivelor, bazelor de date și documentelor EYP.

[163] Ombudsmanul pentru informații, înființat în 2022, este autorizat să investigheze cazurile în care există semne că instituțiile sau agenții de informații abuzează de puterile lor, subminează drepturile și libertățile omului, subminează interesele legitime sau încalcă reglementările privind prelucrarea datelor cu caracter personal în scopuri de securitate sau apărare națională.

[164] Comitetul olandez de supraveghere a serviciilor de informații și securitate (CTIVD) este organismul de supraveghere al serviciilor de informații și securitate. CTIVD efectuează un control atunci când aplică piratarea informatică ca putere de investigare, adică verifică riscurile tehnice suportate și dispozitivele vizate. De asemenea, publică rapoarte despre legalitatea piratării ca putere de investigație. Cu toate acestea, în conformitate cu noua legislație referitoare la "actorii statali cu programe cibernetice„ din 2024, CTIVD are puteri obligatorii limitate în controlul puterilor de piratare. Conform noii legislații, serviciile de informații și securitate pot face apel la o decizie a TIB și CTIVD, iar un judecător se poate pronunța în această privință. Încă nu a fost pronunțată nicio hotărâre. Persoanele care consideră că au fost tratate ilegal sau incorect de către serviciile de informații și securitate pot depune o plângere la ministrul de interne și relații cu Regatul sau la ministrul apărării. Dacă nu sunt mulțumiți de modul în care a fost tratată plângerea lor, pot depune o plângere la CTIVD. Serviciul de reclamații poate emite decizii obligatorii în urma unui comportament ilegal al serviciilor de informații și de securitate.

[165] Consiliul pentru Supraveghere Civilă este înființat pentru a asigura supravegherea civilă a măsurilor de supraveghere a comunicațiilor. Numit de Adunarea Republicii Macedonia de Nord, Consiliul este compus dintr-un președinte și șase membri, al căror mandat este de trei ani și nu poate fi reînnoit. Printre membri se numără trei experți și trei reprezentanți ai organizațiilor neguvernamentale specializate în drepturile omului, securitate și apărare. Consiliul prezintă Adunării un raport anual privind activitățile sale până la sfârșitul lunii februarie a fiecărui an. Consiliul poate acționa din proprie inițiativă sau ca răspuns la plângerile cetățenilor.

Portugalia,[166] **Suedia**.[167] În **Elveția**, în plus față de supravegherea de către un organ de experți,[168] există și auto-supraveghere și control și supraveghere de către executiv[169]. În **Regatul Unit**, regimul de supraveghere include atât organismele de experți, cât și sistemul judiciar.[170] În **Statele Unite**, atât executivul, cât și sistemul judiciar sunt implicate.[171] În **Irlanda**,[172] un control judiciar independent a aplicării legilor relevante este efectuat de un judecător în exercițiu al Înaltei Curți, care este desemnat în acest scop.[173] În **Kârgâzstan**[174] **și Republica Moldova**,[175] controlul aplicării legilor de către organele care desfășoară activități de obținere a informațiilor îi este acordată procuraturii. În **Malta**,[176] **Polonia**[177] și **Serbia**,[178] executivul este implicat în controlul activităților agențiilor de informații.

[166] Consiliul de Supraveghere al Sistemului de Informații al Republicii Portugheze controlează și supraveghează activitatea Secretarului General al Sistemului de Informații și al Serviciilor de Informații, asigurând respectarea Constituției și a legii, cu un accent deosebit pe păstrarea drepturilor, libertăților și garanțiilor. Este compusă din trei cetățeni eminenți, independenți, aleși de Adunarea Republicii, cu o majoritate de 2/3, pentru un mandat de patru ani; Acest organism, printre alte competențe, supraveghează procedura de acces la datele de telecomunicații și de internet și la datele astfel obținute de serviciile de informații. Legea privind sistemul informatic al Republicii Portugheze instituie, de asemenea, o Comisie de supraveghere a datelor, compusă din trei magistrați de la Biroul Procurorului General, numiți și împuterniciți de Procurorul General al Republicii. Comisia pentru controlul datelor este autoritatea publică competentă pentru monitorizarea respectării principiilor și a normelor privind calitatea și păstrarea confidențialității și securității datelor obținute în conformitate cu procedura obligatorie și obligatorie prevăzută de Legea organică nr. 4/2017.

[167] A se vedea nota de subsol 152 de mai sus.

[168] Autoritatea independentă de supraveghere supraveghează activitățile de informații ale FIS, ale agențiilor cantonale de aplicare a legii și ale altor entități și părți terțe mandatate de FIS și monitorizează aceste activități în ceea ce privește legalitatea, caracterul adecvat și eficacitatea acestora. Are acces la toate informațiile și documentele relevante și la toate spațiile utilizate de entitățile supuse supravegherii. Cfr Articolele 76-78 din IntelSA.

[169] Cfr. Articolul 80 din IntelSA.

[170] PIC efectuează un audit detaliat și raportează cu privire la utilizarea competențelor de investigare, în timp ce CPI analizează plângerile privind abuzul de competențe de investigare (a se vedea nota de subsol 152 de mai sus).

[171] Consiliul de supraveghere a confidențialității și libertăților civile (PCLOB) este responsabil pentru revizuirea noilor politici și proceduri implementate de agențiile de informații și efectuează o revizuire anuală a procedurii de apel a Curții de Control al Protecției Datelor, în timp ce FISC și Curtea de Control al Protecției Datelor (DPRC) sunt responsabile pentru asigurarea supravegherii. DPRC oferă un mecanism de despăgubire printr-o revizuire independentă și imparțială a plângerilor specifice depuse de persoane care pretind încălcări ale legii SUA în contextul activităților de informații ale SUA. Deciziile sale sunt obligatorii.

[172] Irlanda nu are o agenție de informații separată. Funcțiile de informații și securitate ale statului sunt responsabilitatea An Garda Síochána și a Forțelor de Apărare.

[173] Judecătorul desemnat este responsabil de supravegherea funcționării legislației și de emiterea rapoartelor anuale în temeiul articolului 8 din Legea din 1993, al articolului 12 din Legea din 2009 și al articolului 12 din Legea din 2011. În practică, aceasta constă în întâlniri anuale cu oficiali din Ministerul Justiției, poliție și alte agenții irlandeze care folosesc competențele de interceptare și păstrare a datelor, precum și o inspecție a înregistrărilor acestora. Rolul de supraveghere este o funcție cu fracțiune de normă a unui judecător. Nu dispune de niciun suport juridic sau tehnic specializat, ceea ce înseamnă că nu există memorie instituțională și depinde de sprijinul entităților auditate. Când Legea privind poliția, securitatea și siguranța comunității din 2024 va intra în vigoare, supravegherea principală va fi atribuită unui examinator independent.

[174] La solicitarea procurorului abilitat, în legătură cu documentele, informațiile și contestațiile cetățenilor primite de Parchet cu privire la încălcări ale legilor în timpul desfășurării activităților de cercetare operațională, precum și în cadrul verificării procedurii stabilite pentru desfășurarea activităților de cercetare operațională și a legalității deciziilor luate în acest sens, Șefii organului care desfășoară activitățile de cercetare operațională prezintă procurorului documentele serviciului operațional care a stat la baza desfășurării acestor activități

[175] Art. 39 din Legea 59/2012: Supravegherea executării legii se efectuează de către procurorii ierarhic superiori pe baza plângerilor depuse de persoane ale căror drepturi și interese legitime au fost încălcate ca urmare a activității speciale sau din oficiu de investigare. Procurorii ierarhic superiori care efectuează controlul au dreptul de a accesa informațiile care constituie secret de stat în modul prevăzut de lege.

[176] Comisarul serviciilor de securitate.

[177] Ministrul de Interne și Administrație supraveghează activitățile nu numai ale poliției, ci și ale unor forțe speciale, cum ar fi Agenția de Securitate Internă (ABW). Această supraveghere executivă include stabilirea direcției strategice și asigurarea faptului că serviciile de securitate acționează în conformitate cu legea. Cu toate acestea, rolul ministrului este mai mult administrativ și mai puțin concentrat pe controlul operațional de zi cu zi. Ministrul justiției are un rol în supravegherea activităților de supraveghere, în special a celor legate de anchetele penale majore.

[178] Ministerul de Interne și Ministerul Apărării supraveghează diferitele servicii de securitate. Aceste departamente au responsabilități de control administrativ și operațional

64. Există un sistem de control parlamentar a activităților agențiilor de informații în **Austria**, **Belgia**, **Bosnia și Herțegovina, Bulgaria, Canada** [179] **, Croația** [180] **, Danemarca, Estonia, Finlanda**[181], **Franța, Germania, Grecia, Italia**[182]**, Kosovo**[183], **Kârgâzstan, Lituania, Luxemburg** [184] **, Republica Moldova, Țările de Jos, Macedonia de Nord**,[185] **Norvegia**,[186] **Polonia**,[187] **România**, **Serbia**,[188] **Republica Slovacia**, [189] **Spania**, [190] **Suedia**, **Elveția**, [191] **Ucraina**, [192] **Regatul Unit**, **Statele Unite**. [193] Linia de demarcație dintre organele de control parlamentare și

[179] Comitetul Parlamentarilor pentru Securitate Națională și Informații (NSICOP) este un comitet de parlamentari cu un mandat foarte larg. Aceasta include revizuirea oricărei activități desfășurate de un departament în legătură cu securitatea națională sau informațiile, cu excepția cazului în care operațiunea este în curs de desfășurare și ministrul competent este de părere că revizuirea ar fi dăunătoare securității naționale. NSICOP prezintă prim-ministrului un raport anual (care este apoi prezentat Parlamentului), care include constatările și recomandările (fără caracter obligatoriu) făcute în anul precedent.

[180] Comisia pentru afaceri interne și securitate națională este împuternicită să efectueze o inspecție directă la fața locului a Agenției de Securitate și Informații și a Agenției Militare de Securitate și Informații. În rest, activitatea sa se bazează pe primirea, examinarea și discutarea rapoartelor agențiilor (rapoarte anuale și rapoarte pe cazuri sau teme specifice). Președintele comisiei trebuie să provină din rândurile celui mai mare partid de opoziție. Comisia emite decizii, concluzii și recomandări fără caracter obligatoriu.

[181] Comitetul de supraveghere a serviciilor de informații asigură punerea în aplicare și caracterul adecvat al operațiunilor de informații, monitorizează și evaluează domeniile de intervenție ale serviciilor de informații, monitorizează și promovează exercitarea efectivă a drepturilor fundamentale și a drepturilor omului în operațiunile de informații, pregătește rapoartele Ombudsmanului pentru informații și prelucrează constatările Ombudsmanului pentru informații cu privire la controla

[182] Articolul 31 din Legea nr. 124/2007: Comisia parlamentară poate obține, chiar și prin derogare de la interdicția prevăzută la articolul 329 din Codul de procedură penală, copii ale actelor și documentelor referitoare la procedurile și investigațiile în curs în fața autorității judiciare sau a altor organe de anchetă, precum și copii ale actelor și documentelor referitoare la investigații parlamentare și anchete.

[183] Responsabilitățile sale includ, printre altele, monitorizarea legalității activității Agenției de Informații, revizuirea rapoartelor Directorului Agenției de Informații privind operațiunile Agenției și rapoartele Inspectorului General, precum și efectuarea de investigații privind activitatea Agenției.

[184] Capitolul 6 din Legea SRE. Comisia parlamentară de supraveghere este informată din oficiu o dată la șase luni cu privire la măsurile de supraveghere și control al comunicațiilor dispuse de Comisia ministerială de informații la cererea agenției de informații de stat. Comisia parlamentară de supraveghere poate efectua, de asemenea, verificări cu privire la cazuri specifice.

[185] Comisia de supraveghere a măsurilor de control al comunicațiilor, prezidată de un reprezentant al principalului partid de opoziție, face apel și la experți tehnici naționali și internaționali, dintre care doi sunt numiți permanent. Principalul obiectiv al Comisiei este de a verifica dacă măsurile de monitorizare a comunicațiilor sunt puse în aplicare în mod legal și eficace. Comisia analizează, de asemenea, raportul anual al procurorului general privind măsurile speciale de investigare pentru a evalua eficacitatea acestor măsuri. Inspecția are loc cel puțin o dată la trei luni, adesea fără preaviz. După fiecare sesiune de monitorizare, Comisia întocmește un raport detaliat cu privire la legalitatea comportamentului observat sau la detectarea abuzurilor. În caz de nereguli sau abuzuri, Comisia este obligată să informeze prompt procurorul și autoritățile competente. În cele din urmă, Comisia prezintă un raport anual Adunării înainte de sfârșitul lunii februarie a fiecărui an.

[186] Comisia parlamentară norvegiană pentru supravegherea serviciilor de informații și securitate (Comisia EOS) are acces deplin la toate informațiile deținute de serviciile de informații, indiferent de clasificarea acestora. Comitetul EOS se poate ocupa de plângerile persoanelor fizice și ale avertizorilor, dar poate investiga și din proprie inițiativă. Dacă, în timpul unui audit, Comitetul EOS constată că supravegherea este ilegală, poate solicita încetarea supravegherii și ștergerea tuturor informațiilor prin depunerea unei petiții la Tribunalul din Oslo (a se vedea secțiunea 7-12 din Legea privind informațiile din 2020). Acesta raportează anual Parlamentului.

[187] Comitetul pentru servicii speciale, care monitorizează și analizează operațiunile desfășurate de Agenția de Securitate Internă (ABW) și Agenția de Informații (AW). Această comisie organizează audieri, examinează rapoartele și se asigură că activitățile serviciilor de securitate se desfășoară în conformitate cu legea și principiile democratice.

[188] Comisia pentru controlul serviciilor speciale de securitate monitorizează, printre altele, constituționalitatea și legalitatea activității serviciilor de securitate și legalitatea aplicării procedurilor și măsurilor speciale de colectare secretă a datelor.

[189] Comisia specială pentru controlul utilizării dispozitivelor informatice (Comisia nu a fost încă înființată în practică, în principal din cauza dezacordurilor politice) este compusă din opt membri, al căror președinte trebuie să fie din opoziție. Acesta efectuează inspecții cel puțin o dată pe an, dar poate face acest lucru în orice moment, din proprie inițiativă și pe plângerea oricărei persoane care pretinde că a fost supusă unei supravegheri ilegale. Competențele Comisiei sunt în esență competențe de control. Membrii săi au dreptul de a intra în incintă, de a accesa registrele și de a obține informații, chiar și informații clasificate, de la autoritățile competente ale statului. Protocoalele inspecțiilor efectuate sunt apoi transmise comisiilor parlamentare competente. În cazul în care comisiile parlamentare respective suspectează că supravegherea a fost efectuată cu încălcarea legii, acestea trebuie să informeze președintele Parlamentului, care apoi informează procurorul general. De două ori pe an, Parlamentul trebuie să examineze în plen rapoartele comisiilor privind stadiul utilizării măsurilor de supraveghere.

[190] "Comisia Secretelor Oficiale" se întrunește în spatele ușilor închise, iar membrii săi sunt supuși unei obligații de confidențialitate.

[191] „Delegarea controlului” și „delegarea finanțelor” au acces deplin și neîngrădit la toate informațiile de care au nevoie pentru a-și îndeplini responsabilitățile de control.

[192] A se vedea articolul 53 din Legea privind informațiile ucrainene. Articolul 53 din Legea privind informațiile din Ucraina.

[193] Comitetul Permanent pentru Informații al Camerei Reprezentanților (HPSCI) și Comitetul Select al Senatului pentru Informații (SSCI) asigură supravegherea de către Congres a activităților de informații, inclusiv a practicilor de supraveghere. HPSCI are responsabilități legislative și de supraveghere asupra programelor, politicilor, bugetelor și operațiunilor comunității de informații, toate acțiunile sub acoperire și colectarea, exploatarea și diseminarea informațiilor umane. CISS asigură supravegherea legislativă a activităților de informații ale guvernului SUA. Aceasta include desfășurarea de audieri cu oficiali de rang înalt ai agențiilor de informații, efectuarea de investigații și revizuirea programelor de informații și revizuirea și colectarea activităților/analizelor de informații.

independente/experți nu este rigidă, deoarece există organe „hibride” (a se vedea, de asemenea, paragraful 117 de mai jos).

65. În **Cipru** și **Portugalia**, comisiile parlamentare nespecializate participă la controlul activităților agențiilor de informații.

F. Notificarea măsurilor de supraveghere țintită

66. În cele din urmă, Comisia de la Veneția a analizat existența unui mecanism de notificare post-supraveghere în cadrul executării măsurilor de supraveghere țintită. În cadrul procedurilor penale, existența unui mecanism de notificare a măsurilor de supraveghere specifice a fost raportată de **Bosnia și Herțegovina**,[194] **Canada**,[195] **Danemarca**, [196] **Estonia**, [197] **Finlanda**, [198] **Germania**, [199] **Grecia**, [200] **Italia**, [201] **Coreea**,[202] **Kârgâzstan**, **Liechtenstein**,[203] **Lituania**,[204] **Luxembourg**,[205] **Republica Moldova**,[206] **Țările de Jos**,[207] **Macedonia de Nord**,[208] **San Marino**,[209] **Serbia**,[210] **Republica Slovacia**,[211] **Elveția**,[212] **Ucraina**[213]. În lipsa exigențelor de notificare, pot fi depuse plângeri pentru măsurile dispuse sau efectuate cu încălcarea dispozițiilor legale în **Austria,**[214] **Irlanda**.[215] Utilitatea notificării ca remediu depinde de modul în

[194] articolul 119 din Codul de procedură penală, cu posibilitatea de a solicita instanței să examineze legalitatea ordonanței și modul în care a fost pusă în aplicare măsura.
[195] Articolele 196 și 196.1 din Codul penal prevăd obligația de a informa în scris, după fapt, persoanele ale căror comunicări private au fost interceptate în temeiul unei autorizații sau în situații de urgență fără mandat, atunci când există un risc iminent de vătămare.
[196] Articolul 788 din Legea privind administrarea justiției: Notificarea trebuie făcută cât mai curând posibil în cazul în care poliția, în termen de 14 zile de la expirarea perioadei pentru care a fost autorizată intervenția, nu a acționat în urma notificării. Excepție fac cazurile în care ar fi în detrimentul investigației sau al investigației într-o altă cauză pendinte privind o infracțiune care, potrivit legii, poate constitui baza unei ingerințe în secretul comunicațiilor sau dacă protecția informațiilor confidențiale despre metodele sau circumstanțele de investigație ale poliției împiedică notificarea. În aceste cazuri, instanța poate, la cererea poliției, să decidă ca notificarea să fie omisă sau amânată pentru o perioadă determinată, care poate fi prelungită printr-o hotărâre ulterioară.
[197] Articolul 126 alineatul 13 din Codul de procedură penală.
[198] Articolul 60 din Legea privind măsurile coercitive prevede notificarea utilizării măsurilor coercitive secrete.
[199] Articolul 101 din Codul de procedură penală.
[200] În materie penală, după expirarea măsurii și la depunerea unei cereri relevante din partea părții afectate, ADAE notifică partea afectată cu privire la impunerea acestei măsuri în termen de șaizeci (60) de zile, cu acordul procurorului Curții Supreme și cu condiția ca scopul pentru care a fost dispusă măsura să nu fie compromis (art. 6 din Legea nr. 5002/2022).
[201] Articolele 268 și 269 din Codul de procedură penală
[202] În termen de 30 de zile de la data încetării măsurilor.
[203] Articolul 104 § 2 din Codul de procedură penală (StPO). Artă. 104 § 4 StPO prevede, de asemenea, că o cale de atac poate fi depusă la Curtea Superioară în termen de paisprezece zile de la notificarea de către judecătorul de instrucție. Această decizie poate face obiectul unei plângeri individuale la Curtea Constituțională
[204] Articolul 161 din Codul de procedură penală
[205] articolul 88-4 § 6 din Codul de procedură penală; De asemenea, aceștia sunt informați că pot introduce o acțiune în anulare în temeiul și în condițiile prevăzute la articolul 126
[206] Notificarea poate fi amânată până la sfârșitul urmăririi penale. Articolul 313 din Codul de procedură penală prevede o cale de atac împotriva acțiunilor și actelor ilegale ale Parchetului și ale organelor speciale de anchetă
[207] Articolul 126b din Codul de procedură penală. Notificarea sau comunicarea trebuie să aibă loc cât mai curând posibil, dar nu are loc atunci când este „imposibil în mod rezonabil” sau atunci când persoanele sunt notificate automat în contextul procedurilor penale în curs.
[208] Articolul 262 din Codul de procedură penală.
[209] Legea nr. 98 din 21 iulie 2009.
[210] Articolul 163 din Codul de procedură penală
[211] Articolele 114 și 115 din Codul de procedură penală: Persoanele în cauză care nu au acces la dosar trebuie să fie informate, în termen de trei ani de la pronunțarea hotărârii definitive în cauza penală, că au fost monitorizate și că înregistrările au fost distruse. Aceștia trebuie să fie informați cu privire la posibilitatea de a depune o petiție la Curtea Supremă pentru o revizuire a mandatului judiciar care autorizează supravegherea.
[212] Articolul 279 din Codul de procedură penală: motivele, tipul și durata supravegherii cel târziu la sfârșitul procedurii preliminare. Tribunalul pentru măsuri obligatorii poate amâna sau renunța la notificare în cazul în care rezultatele nu sunt utilizate ca probe în cadrul procedurilor judiciare și în cazul în care amânarea sau omisiunea este necesară pentru a proteja interesele publice sau private preponderente.
[213] Legea nr. 98 din 21 iulie 2009.
[214] Articolul 106 § 1 din Codul de procedură penală.
[215] Articolul 9 din Legea din 1993, articolul 11 din Legea din 2009 și articolul 10 din Legea din 2011 permit unei persoane să se adreseze unui arbitru de soluționare a plângerilor pentru a analiza dacă a fost acordată o autorizație ministerială de interceptare și, în caz afirmativ, dacă cerințele legii relevante au fost îndeplinite în ceea ce privește cererea. Terțul care se pronunță în cadrul procedurii sumare poate examina legalitatea măsurilor luate. El este numit de Taoiseach pentru un mandat de cinci ani. Până

care excepțiile de la aceasta sunt interpretate în practică (a se vedea ăaragrafele 120-122 de mai jos).

67. Următoarele țări au raportat un sistem de notificare în cazurile de supraveghere țintită efectuată de serviciile de securitate: **Belgia**[216]**, Bosnia și Herțegovina**[217]**, Danemarca**[218]**, Estonia**[219]**, Finlanda**[220]**, Germania**[221]**, Coreea**[222]**, Republica Moldova**[223]**, Olanda**[224]**, Macedonia de Nord**[225]**, România**[226]**, Elveţia**[227]**, Ucraina**[228].

acum, toți deținătorii acestei funcții au fost judecători în exercițiu la Curtea de Circuit. Arbitrul are puterea de a accesa toate documentele oficiale referitoare la măsurile luate. În cazul în care concluzionează că legea a fost încălcată, trebuie să informeze solicitantul în scris și să raporteze Taoiseach. De asemenea, poate anula o autorizație ministerială, poate ordona agenției în cauză să distrugă informațiile obținute și poate recomanda despăgubiri. Sistemul de despăgubire se limitează la verificarea dacă un mandat a fost emis corect și nu prevede recurs în alte situații, cum ar fi păstrarea sau divulgarea necorespunzătoare a datelor de către serviciile de telecomunicații sau utilizarea abuzivă a datelor de către Gardaí.

[216] Astfel cum se prevede la articolul 2 § 3 din R&S.A., condițiile sunt următoarele: a trecut o perioadă mai mare de zece ani de la încheierea metodei. Condițiile sunt, printre altele, că a trecut o perioadă mai mare de zece ani de la încheierea metodei, că notificarea nu poate aduce atingere unei investigații de informații și că nu poate aduce atingere relațiilor dintre Belgia și instituțiile internaționale sau supranaționale străine.

[217] Articolul 77 din Legea privind Agenția de Informații și Securitate, după încheierea inspecției, cu excepția cazului în care aceste informații pot pune în pericol îndeplinirea sarcinilor agenției sau finalizarea procedurii în fața autorităților competente.

[218] A se vedea nota de subsol 196 de mai sus.

[219] Articolul 29 din Legea privind autoritățile de securitate: excepțiile sunt următoarele: (1) încalcă în mod semnificativ drepturile și libertățile altei persoane garantate de lege sau pune în pericol o altă persoană; 2) pune în pericol confidențialitatea mijloacelor, metodelor sau tacticilor autorității de securitate; 3) pune în pericol sursa de informații sau o persoană recrutată pentru cooperare sub acoperire; (4) să afecteze schimbul de informații între autoritățile de securitate sau cooperarea cu un stat străin sau o organizație internațională

[220] Articolul 20 din Legea privind utilizarea informațiilor privind traficul de rețea în informațiile civile și articolul 89 din Legea privind informațiile militare

[221] Articolul 59 din Legea privind Serviciul Federal de Informații și articolul 12 din Legea privind articolul 10

[222] A se vedea nota de subsol 202 de mai sus.

[223] Articolul 22 din Legea nr. 59/2012, cu următoarele excepții: a) informațiile constituie un risc crescut pentru viața și sănătatea persoanei; (b) este necesar să se efectueze o altă măsură specială de investigare în același caz special; (c) rezultatele măsurii speciale de investigare necesită urmărire penală. Articolul 26 din Legea nr. 59/2012 prevede un mecanism de recurs

[224] Articolul 59 alineatul (1) din Legea privind serviciile de informații și de securitate. În principiu, persoanele vizate de aplicarea unei competențe de investigare trebuie să fie informate la cinci ani de la încetarea competenței de investigare. Notificarea nu este necesară atunci când (a) sunt dezvăluite surse dintr-un serviciu, inclusiv serviciile de informații și de securitate ale altor țări; (b) relațiile cu alte țări și cu organizațiile internaționale sunt grav compromise; sau (c) o aplicare specifică a unei metode (modus operandi) sau identitatea persoanei care a asistat serviciul în aplicarea metodei este dezvăluită

[225] Articolul 51 alineatul (6) din Legea privind supravegherea comunicațiilor impune Consiliului de Control Civil să informeze imediat cetățeanul dacă este detectat un abuz în timpul supravegherii. Dacă nu se observă niciun abuz, cetățeanul este întotdeauna informat, dar cu detalii limitate pentru a păstra confidențialitatea

[226] Articolul 21 § 2 din Legea nr. 51/91 privind securitatea națională a României. Notificarea este exclusă dacă (a) ar putea duce la compromiterea îndeplinirii funcțiilor oficiale ale organelor de stat responsabile de securitatea națională prin dezvăluirea surselor acestora, inclusiv a celor ale serviciilor de securitate și de informații ale altor state; (b) ar putea afecta apărarea securității naționale; c) ar putea încălca drepturile și libertățile terților; (d) ar putea conduce la divulgarea metodelor și mijloacelor, inclusiv a tehnicilor specifice de investigare, utilizate în cazul în cauză de către organele statului responsabile cu securitatea națională.

[227] În cazul în care ținta este situată în Elveția, articolul 33 din IntelSA prevede că persoana monitorizată trebuie să fie informată în termen de o lună de la încheierea tranzacției. Excepțiile sunt următoarele: a. amânarea este necesară pentru a nu pune în pericol o anchetă sau o procedură judiciară în curs; b. amânarea este necesară din cauza unui alt interes public superior în menținerea securității interne sau externe sau din cauza relațiilor Elveției cu alte țări; c. informațiile ar putea pune în pericol terți; d. persoana în cauză nu este contactabilă. În cazul în care persoana în cauză se află în străinătate, aceasta nu este informată cu privire la măsura de informații

[228] Articolul 25 din Legea Ucrainei "Cu privire la informații", prevedea că furnizarea unor astfel de informații nu constituie o amenințare la adresa securității naționale a Ucrainei

68. În **Canada**, **Grecia**,[229] **Irlanda**[230],[3] **Kosovo**,[231] **Kârgâzstan**, **Slovacia**[232], **Statele Unite**[233]**,** deși nu există nicio obligație de notificare în contextul operațiunilor de informații, plângerile pot fi depuse la organele/instanțele de control competente.

G. Prezentare generală a legislaţiei şi a practicii anumitor state în scopul prevenirii abuzului de programe spion

69. Trebuie notat faptul că în unele state au fost întreprinse măsuri legislative specifice pentru a limita dezvoltarea programelor spion sau pentru a reacționa la acuzațiile de utilizare abuzivă.

70. În **Austria**, Curtea Constituțională a considerat la 11 decembrie 2019[234] că monitorizarea secretă a utilizării sistemelor informatice a constituit o ingerință gravă în dreptul la viață privată protejat de articolul 8 din Convenția Europeană a Drepturilor Omului (CEDO) și era permisă numai în cadrul unor limite extrem de restrânse pentru a proteja interese juridice la fel de importante.[235] Prin urmare, ea a declarat neconstituțională articolul 135a din Codul de procedură penală, adoptat în 2018, care permitea utilizarea programelor spion pentru a citi mesaje criptate. Articolul 135a coroborat cu articolul 134 § 3a din Codul de procedură penală prevedea (în cazuri precise și în anumite condiții) pentru o autorizație de a monitoriza în secret mesajele criptate prin instalarea unui program spion - un așa-numit „Troian Federal” (Bundestrojaner) - pe un sistem informatic. Cu toate acestea, aceste dispoziții nu au

[229] În aprilie 2024, Consiliul de Stat al Greciei a declarat neconstituțional un amendament legislativ din 2021 care interzicea ADAE să informeze cetățenii despre supravegherea statului din motive de "securitate națională". Consiliul de Stat a constatat că interdicția generală de a informa persoanele cu privire la faptul că au fost supuse supravegherii a constituit o "restricție nejustificată" a dreptului la viață privată și o amenințare la adresa statului de drept. Datorită modificărilor legislative aduse în 2022, în temeiul articolului 4 alineatul (3) din Legea nr. 5002/2022, persoanele interesate, în cazul în care suspectează că au fost vizate, trebuie să se adreseze ADAE, care o depune apoi la PEJ. Cu toate acestea, legea prevede că aceste cereri sunt admisibile numai după o perioadă de trei ani de la încheierea supravegherii. Nici ADAE, nici PEJ nu pot decide în această privință, ci o comisie formată din trei membri, compusă din procurorul PEJ, al doilea procuror de rang înalt responsabil de dosar și președintele ADAE. Comisia poate da curs cererii numai în cazul în care consideră că divulgarea nu compromite domeniul de aplicare pentru care a fost impusă monitorizarea specifică. Mai important, în cazul în care comisia decide să notifice persoana în cauză, legea prevede că nu i se comunică informații suplimentare, cu excepția faptului că comunicările sale au fost interceptate în perioada dezvăluită. Cu toate acestea, nu toate informațiile despre motivul pentru care a fost impusă supravegherea sunt dezvăluite.

[230] A se vedea nota de subsol 215 de mai sus

[231] Articolul 39 alineatul (2) din Legea privind Agenția de Informații din Kosovo prevede că persoanele fizice, instituțiile și părțile terțe au dreptul de a depune o plângere împotriva Agenției de Informații din Kosovo la instituția Ombudsmanului.

[232] Persoanele afectate pot, de asemenea, să depună o plângere constituțională în temeiul articolului 127 din Constituție. 127 din Constituție. Mecanismul constituțional de plângere s-a dovedit recent esențial pentru a umple un gol în PAIA, și anume că instanțele regionale care exercită controlul judiciar în temeiul PAIA nu au puterea de a ordona în mod specific distrugerea înregistrărilor obținute prin supraveghere ilegală. Această omisiune legislativă a fost criticată de Curtea Europeană a Drepturilor Omului în hotărârea sa din 2021 în cauza Zoltán Varga v. Slovacia, nr. 58361/12 și alte 2, 20 iulie 2021. În recenta hotărâre din 15 mai 2024 (III. ÚS 97/2012), Curtea Constituțională a dispus în mod expres - în acest caz - Serviciul de Informații din Slovacia să distrugă toate înregistrările și alte documente încă existente obținute prin supravegherea ilegală efectuată în acest caz și să informeze reclamantul cu privire la distrugerea acestora.

[233] FISA prevede căi de atac individuale în cazul actelor ilegale comise de funcționari publici împotriva persoanelor vizate. ECPA prevede o acțiune de ștergere în cazul interceptării comunicațiilor electronice și orale. În cele din urmă, în fața Curții de Revizuire a Protecției Datelor, persoanele pot depune plângeri cu privire la presupuse încălcări ale activității de supraveghere a guvernului SUA în timpul colectării sau procesării datelor unei persoane.

[234] Curtea Constituțională, Culegere de decizii 20356/2019 (11 decembrie 2019).

[235] Curtea Constituțională a constatat că "calul troian federal" a fost o formă deosebit de intruzivă de măsură de supraveghere, nu în ultimul rând pentru că o imagine de ansamblu a datelor obținute prin supravegherea unui sistem informatic a permis tragerea de concluzii, printre altele, cu privire la preferințele personale și stilul de viață al utilizatorilor individuali. În plus, (a) a afectat un număr mare de persoane; (ii) nu exista nicio garanție că măsura de monitorizare va fi pusă în aplicare numai dacă va fi utilizată pentru urmărirea penală și soluționarea infracțiunilor suficient de grave; (iii) măsura nu a asigurat în mod adecvat protecția vieții private a persoanelor afectate de calul troian; și (iv) nu exista nicio garanție că, după aprobarea judiciară ex ante a măsurii, ofițerul de protecție juridică va fi în măsură să monitorizeze în mod eficient și independent orice supraveghere sub acoperire în curs de desfășurare.

intrat niciodată în vigoare, deoarece la 11 decembrie 2019, Curtea Constituțională a Austriei le-a anulat.

71. Diferite forme de evaluare a utilizării programelor spion, inclusiv prin comisii de anchetă, au avut loc în **Belgia**,[236] **Canada**,[237] **Grecia**,[238] **Italia**[239], **Țările de Jos**,[240] **Polonia**,[241] **Spania**,[242] **Suedia**,[243] **Elveția**,[244] **Statele Unite**.[245]

[236] Investigație de control în urma dezvăluirilor privind utilizarea software-ului PEGASUS, citate mai sus.

[237] Comisia permanentă pentru accesul la informații, confidențialitate și etică a Camerei Comunelor a pregătit un raport privind instrumentele de investigație bazate pe dispozitive utilizate de Poliția Regală Canadiană (RCMP) și problemele conexe, menționate mai sus. Raportul examinează beneficiile și riscurile utilizării instrumentelor de investigare a dispozitivelor și examinează măsurile legislative și non-legislative care ar putea fi luate în considerare pentru a reglementa mai bine aceste tipuri de instrumente în Canada. Raportul a constatat că există un decalaj legislativ în ceea ce privește utilizarea noilor instrumente tehnologice de investigare. Prin urmare, concluzionează că este necesar un cadru legislativ mai bun pentru utilizarea de către RCMP a instrumentelor de investigație bazate pe dispozitive pentru a asigura utilizarea adecvată a acestor instrumente și protecția drepturilor la viață privată ale canadienilor.

[238] În urma incidentelor raportate în 2022 (a se vedea raportul APCE, citat mai sus, expunere de motive, §§ 31-35), a fost efectuată o anchetă parlamentară oficială pentru a examina orice acuzații de utilizare a programelor spion ilegale în scopuri oficiale. Comisia a examinat modul în care serviciile naționale de informații, ca parte a rolului lor, ar putea desfășura operațiuni de supraveghere autorizate legal, prin mijloace proporționale și convenționale. Concluziile comisiei au fost puse la dispoziția tuturor membrilor Parlamentului grec, sub sigiliul confidențialității.

[239] Document aprobat de Comisia a 2-a permanentă (Justiție) în ședința sa din 20 septembrie 2023 la încheierea anchetei de constatare a faptelor privind problema interceptărilor convorbirilor telefonice, citat anterior, p. 41 și sf.

[240] În 2022, Centrul de cercetare și date al Ministerului Justiției și Securității din Țările de Jos a publicat un raport de evaluare privind utilizarea programelor spion de către autoritățile de aplicare a legii. Acesta este un studiu empiric al implementării acestei puteri. Studiul a constatat că, între martie 2019 și martie 2021, puterea a fost emisă în 26 de anchete penale. Acesta a fost utilizat în anchete penale privind forme mai grave de criminalitate tradițională, cum ar fi tentativa de omor, cazuri care implică narcotice, falsificarea documentelor, spălarea banilor, infracțiuni sexuale, infracțiuni de terorism și apartenența la o organizație criminală. Raportul afirmă că poliția olandeză a folosit un instrument comercial în "marea majoritate" a cazurilor. În contextul serviciilor de informații și securitate, în 2020 a fost evaluată întreaga lege privind serviciile de informații și securitate, inclusiv utilizarea spyware-ului la articolul 45. Cu toate acestea, accentul nu a fost pus pe "supravegherea țintită", ci mai degrabă pe utilizarea programelor spion îndreptate către organizații și pe achiziționarea de seturi de date în vrac. Numele instrumentelor de afaceri utilizate nu este public.

[241] În februarie 2024, a fost înființată o comisie parlamentară specială pentru a investiga utilizarea programelor spion, despre care ministrul polonez al justiției a spus că a fost folosit pe aproape 600 de persoane între 2017 și 2022. La 10 septembrie 2024, Curtea Constituțională poloneză a decis că comisia este neconstituțională în contextul activității sale.

[242] În urma dezvăluirilor potrivit cărora 65 de persoane au fost vizate (în așa-numitul „CatalanGate") de programe spion (Raportul APCE, citat mai sus, Expunere de motive, §§ 36-42), a fost înființată o comisie specială de anchetă: Comisia parlamentară de anchetă privind spionajul și intruziunea în viața privată și intimitate, prin intermediul programelor malware Pegasus și Candiru, lideri politici, activiști, avocați, jurnaliști, instituții și familiile și cei dragi. *Comisión de Investigación sobre el espionaje e intromisión a la privacidad e intimidad, a través de los malware Pegasus y Candiru, a líderes políticos, activistas, abogados, periodistas, instituciones y sus familiares y allegados.* Comisia are competența de a examina în detaliu implicarea instituțiilor statului în presupuse ingerințe ilegale împotriva liderilor politici, a instituțiilor și a altor persoane; (b) să investigheze presupusa responsabilitate și utilizarea abuzivă a agențiilor tehnice din toate departamentele ministeriale și legătura acestor agenții cu spionajul; c) să examineze în detaliu toate activitățile Ministerului Afacerilor Externe în legătură cu investigațiile efectuate într-o manieră presupus ilegală, fără a fi subestimată, de către delegațiile Generalității în străinătate; d) să fie la curent cu contractele, costurile și procedurile de achiziții pentru presupusa dezvoltare și/sau achiziționare a programului Pegasus sau a altor instrumente utilizate pentru spionaj de către organismele oficiale; e) să investigheze toate inițiativele autorităților de stat de a persecuta disidența politică; f) să propună și să ridice măsuri reparatorii pentru toți cei afectați de investigații ilegale, precum și tragerea la răspundere pentru utilizarea abuzivă a aparatului guvernamental; și (g) să propună măsuri adecvate de monitorizare, investigare și prevenire pentru a proteja democrația împotriva abuzurilor puterii de stat și pentru a preveni utilizarea acesteia împotriva drepturilor civile și politice. O a doua comisie, Comisia parlamentară de anchetă "privind așa-numita "Operațiune Catalonia" și acțiunile Ministerului de Interne în timpul guvernelor Partidului Popular în legătură cu presupusele nereguli care leagă înalți oficiali și comandanți de poliție de existența unei conspirații de autoapărare" este competentă, printre altele, să „cunoască contractele, cheltuielile și procedurile de achiziții pentru dezvoltare și/sau achiziție presupus software numit „Pegasus" sau alte instrumente presupuse folosite pentru spionaj de către organisme oficiale".

[243] Autorizația inițială de utilizare a programelor spion a fost precedată de o comisie de anchetă (așa cum este norma pentru toate noile legislații din Suedia) - Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet, SOU 2017:89. Legea introdusă în 2020 urma să se aplice pentru o perioadă limitată de timp (până în martie 2025). În 2023, funcționarea legii a fost examinată de o altă comisie de anchetă, Hemlig dataavläsning - utvärdering och permanent lagstiftning, SOU 2023:78. Concluzia generală a acestei a doua comisii de anchetă a fost că legea, deși a fost aplicată doar pentru o perioadă scurtă de timp, a fost folosită mai mult decât s-a intenționat și că a fost un instrument esențial de investigație care ar trebui să devină permanent.

[244] Comisia parlamentară competentă a solicitat din 2019 un raport anual de performanță din partea FIS în conformitate cu articolul 26 din Legea privind securitatea internă și măsurile împotriva sistemelor informatice străine în conformitate cu articolul 37 din Legea privind securitatea internă. În raportul său, CRS oferă o evaluare cuprinzătoare a beneficiilor măsurilor și abordează aspectele tehnice și aspectele legate de resurse. Statisticile arată că 9 operațiuni au folosit un program special pentru calculator în 2023, comparativ cu 7 în anul precedent.

[245] Statele Unite au evaluat programul spion comercial și au concluzionat, în Ordinul executiv al Casei Albe privind interzicerea utilizării de către guvernul Statelor Unite a programelor spion comerciale care prezintă riscuri pentru securitatea națională, 27 martie 2023, că „exploatarea tot mai mare a datelor sensibile ale americanilor și utilizarea necorespunzătoare a tehnologiilor de supraveghere, inclusiv program spion comercial, amenință dezvoltarea" unui „ecosistem" tehnologic internațional [...]. În ceea ce privește securitatea națională și interesele de politică externă, decretul notează că este util „să ne asigurăm că tehnologia este dezvoltată, implementată și gestionată în conformitate cu drepturile universale ale omului, statul de drept și autorizațiile, garanțiile și controalele legale adecvate, astfel încât să sprijine și să nu submineze democrația, libertăți civile și siguranță publică".

72. **Statele Unite** au adoptat legi care impun restricții asupra Pegasus și a categoriilor conexe de programe de spion comerciale. Legea publică 117-263 (50 USC §3232a) (2022)[246] le impune agențiilor de informații americane să furnizeze rapoarte anuale de evaluare a amenințărilor de contra-spionaj „și a altor riscuri la adresa securității naționale" pe care „programele spion comerciale străine" le prezintă Națiunilor Unite. De asemenea, ea autorizează directorul Serviciului Național de Informații să interzică agențiilor de informații să „încheie un contract sau alt acord în orice scop cu o companie care a achiziționat, în totalitate sau parțial, un program spion comercial străin." Legea publică 117-81 (22 USC §2679e) (2021)[247] îi solicită Secretarului de Stat să pregătească o listă de contractanți care „au asistat sau au facilitat în mod conștient un atac cibernetic sau au efectuat o supraveghere" împotriva Statelor Unite sau împotriva: „*[i] persoanelor, inclusiv activiști, jurnaliști, politicieni din opoziție sau alte persoane, în scopul suprimării disidenței ori de a intimida criticii, în numele unei țări incluse în rapoartele anuale ale departamentului privind practicile în materia drepturilor omului pentru acte sistematice de represiune politică, inclusiv arestări sau detenții arbitrare, tortură, execuții extrajudiciară sau motivate politic sau alte încălcări flagrante ale drepturilor omului".* Decretul 14093,[248] promulgat în temeiul unei astfel de autorizații, îi interzice oricărei agenții federale sau departament să utilizeze în mod operațional programele spion comerciale atunci când determină, printre altele „că programul spion comercial prezintă riscuri semnificative de utilizare necorespunzătoare de către un guvern străin sau de către o persoană străină." Decretul precizează în continuare bazele pe care o agenție s-ar putea fundamenta pentru a lua o astfel de decizie, inclusiv utilizările care încalcă dreptul internațional al drepturilor omului.

73. Trebuie notat faptul că guvernele din Australia, Austria, Canada, Costa Rica, Danemarca, Estonia, Finlanda, Franța, Germania, Japonia, Lituania, Olanda, Noua Zeelandă, Norvegia, Polonia, Polonia, Republica Irlanda, Republica Coreea, Suedia, Elveția, Regatul Unit, iar Statele Unite au aprobat o declaraţie comună care angajează semnatarii să lucreze împreună pentru a contracara proliferarea şi utilizarea abuzivă a programelor spion cu utilizare comercială.[249] În special, părțile se angajează să colaboreze pentru a contracara utilizarea abuzivă a programelor spion și: (i) să depună eforturi pentru a institui balustrade și proceduri solide pentru a se asigura că orice utilizare comercială a programelor spion este compatibilă cu respectarea drepturilor universale ale omului, a statului de drept, a drepturilor civile și a libertăților civile; (ii) să prevină exportul de programe, tehnologii și echipamente către utilizatorii finali care sunt susceptibili să le utilizeze pentru activități cibernetice rău-intenționate; (iii) să ditribuie informații privind proliferarea și utilizarea abuzivă a programelor spion comerciale; (iv) să colaboreze strâns cu partenerii industriali și cu grupurile societății civile pentru a-și ilumina abordarea, a contribui la creșterea gradului de conștientizare și a stabili standarde adecvate, continuând totodată să sprijine inovarea; (v) să implice alte guverne guvernelor partenere din lume pentru a alinia mai bine politicile și autoritățile de control al exporturilor pentru a atenua în mod colectiv utilizarea abuzivă a programelor spion comerciale și a încuraja reforma în acest sector.

[246] Disponibil aici.
[247] Disponibil aici.
[248] Ordin executiv privind interzicerea utilizării de către guvernul Statelor Unite a programelor spion comerciale care prezintă riscuri pentru securitatea națională, citat mai sus.
[249] Casa Albă, Declarație comună privind eforturile de contracarare a proliferării și utilizării abuzive a programelor spion comerciale, 18 martie 2024. Lista statelor, astfel cum a fost modificată ultima dată la 22 septembrie 2024.

V. Garanții minime împotriva abuzurilor de putere

74. După cum s-a observat mai sus, este esențial să se asigure că utilizarea programelor spion nu le oferă statelor o putere arbitrară și ilegală de a interfera cu viața privată a persoanelor.[250] Statele sunt obligate să respecte obligațiile prevăzute de dreptul internațional cutumiar, precum și obligațiile pe care și le-au asumat prin aderarea la tratatele internaționale privind drepturile omului, cum ar fi CEDO (și PIDCP), care urmăresc protejarea drepturilor omului și respectarea statului de drept. Pentru ca supravegherea prin utilizarea programelor spion să fie compatibilă cu articolul 8 din CEDO și cu articolul 17 din PIDCP, cadrul juridic care o autorizează trebuie să corespundă unor exigențe foarte stricte. Bazându-se pe jurisprudența Curții Europene în materia supravegherii țintite, rapoartele anterioare ale Comisiei de la Veneția, alte standarde europene și internaționale, cum ar fi Convenția 108+, precum și analiza comparativă a legislației relevante în statele membre ale Comisiei de la Veneția, această secțiune oferă o imagine de ansamblu neexhaustivă a principiilor majore care ar trebui să fie respectate atunci când se utilizează programe spion pentru a se conforma standardelor statului de drept și drepturilor omului.

A. Legislație primară accesibilă și previzibilă

75. Având în vedere că utilizarea programelor spion constituie o ingerință în dreptul la respectarea vieții private, așa cum este ilustrat mai sus, Articolul 8 alin. (2) din CEDO și articolul 17 din PIDCP prevăd că aceasta poate fi autorizată numai dacă este reglementată în mod corespunzător prin lege, și anume că este „conformă cu legea”. Potrivit Curții Europene, acest lucru „nu doar necesită ca măsura contestată să aibă o bază în dreptul intern, ci se referă și la calitatea legii în cauză, implicând ca acesta să fie accesibilă persoanei în cauză și previzibilă în ceea ce privește efectele sale”.[251]

76. Curtea Europeană a declarat că, având în vedere riscul de abuz inerent oricărui sistem de supraveghere secretă, astfel de măsuri trebuie să se bazeze pe o lege deosebit de precisă, mai ales că tehnologia disponibilă pentru utilizare devine din ce în ce mai sofisticată.[252] Astfel, utilizarea unui instrument special de investigare, cum ar fi programul spion, trebuie reglementată de legislația *primară*, adică de o lege.[253] O astfel de cerință are avantajul legitimității democratice, deoarece permite unui legislator ales în mod democratic să determine echilibrul exact care ar trebui să fie stabilit între interesele concurente și consolidează securitatea juridică.[254] În plus, legea trebuie să îndeplinească cerințele de calitate: ea trebuie să fie accesibilă persoanelor vizate și previzibilă în ceea ce privește efectele sale.

[250]Comisia de la Veneția, CDL-AD(2016)007, citată mai sus, § 118.
[251] Curtea Europeană, Rotaru v. România [MC], nr. 28341/95, 4 din 2000, - 52.
[252] Curtea Europeană, Uzun v. Germania, nr. 35623/05, 2 septembrie 2010, § 61.
[253] A se vedea, mutatis mutandis, Curtea Europeană a Drepturilor Omului, Hotărârea Bykov v. Rusia [MC], nr. 4378/02, 10 martie 2009, §76.
[254] În Suedia, de exemplu, s-a considerat necesar să se impună o obligație legală de a documenta toate deciziile luate în contextul măsurilor secrete de investigare. Nu s-a considerat suficient ca aceste chestiuni să fie reglementate de instrucțiuni interne din partea parchetului sau a poliției/poliției de securitate. Vezi prop. 2022/23:126, p. 181.

77. Având în vedere cele de mai sus, calitatea dreptului intern care reglementează utilizarea programelor spion este o condiție prealabilă esențială pentru reducerea interferenței programelor spion cu drepturile la viață privată și la protecția datelor (și a altor drepturi ale omului), precum și pentru limitarea riscului de abuz de putere. În cazul în care statele decid să utilizeze o astfel de tehnică de supraveghere, le-ar reveni o obligație pozitivă de a prevedea conformitatea cadrului legislativ cu exigențele de „calitate" a dreptului prevăzute, în special, la articolul 8 din CEDO.

1. *Accesibilitatea legislației*

78. În statele în privința cărora Comisia deține informații, legea care reglementează supravegherea țintită ar fi, de obicei, o dispoziție a codului de procedură penală sau un act legislativ primar specific consacrat competențelor de supraveghere/investigație.[255] Acestea sunt acte publicate oficial, accesibile publicului.

2. *Previzibilitatea legislației*

79. Potrivit Curții Europene, o regulă este „previzibilă" dacă este formulată cu suficientă precizie pentru a-i permite oricărei persoane – după caz, cu consiliere adecvată - să-și adapteze conduita. Această cerință de precizie constituie o garanție esențială împotriva arbitrarului în impunerea măsurilor restrictive, iar o astfel de protecție este și mai importantă în ceea ce privește măsurile de supraveghere secretă, din cauza riscurilor sporite de arbitrariu în astfel de circumstanțe.[256]

80. Cu toate acestea, în contextul special al supravegherii, previzibilitatea nu înseamnă că persoanele ar trebui să poată prevedea momentul în care autoritățile sunt susceptibile să intercepteze comunicațiile lor, astfel încât să își poată adapta comportamentul în consecință.[257] În contextul supravegherii menite să facă faţă ameninţărilor la adresa securităţii naţionale, caracterul vag al conceptului de securitate naţională creează probleme particulare, deoarece o reglementare eficientă necesită un nivel ridicat de precizie, și o reglementare eficientă este o condiție prealabilă pentru un control eficient.

81. Cu toate acestea, Curtea Europeană a constatat că cerința de „previzibilitate" a legii nu merge atât de departe încât să oblige statele să adopte dispoziții legale care să enumere în detaliu toate comportamentele care ar putea determina o decizie de a supune o persoană supravegherii secrete pe motive de „securitate națională". Prin natura lor, amenințările la adresa securității naționale pot varia în funcție de natura lor și pot fi imprevizibile sau dificil de definit în prealabil.[258] În același timp, Curtea Europeană a subliniat, de asemenea, că în chestiuni care afectează drepturile fundamentale, ar fi contrar statului de drept, unul dintre principiile de bază ale unei

[255] A se vedea printre altele Legea din 2016 privind competențele de investigare din Regatul Unit
[256] Curtea Europeană a Drepturilor Omului, Malone v. Regatul Unit, nr. 8691/79, 2 august 1984, § 68: „Deoarece aplicarea supravegherii secrete a comunicațiilor este în afara controlului atât al părților implicate, cât și al publicului, „legea" ar fi contrară statului de drept dacă puterea discreționară acordată executivului nu ar cunoaște limite. În consecință, acesta trebuie să definească domeniul de aplicare și modul în care o astfel de competență este exercitată cu suficientă claritate - având în vedere scopul legitim urmărit - pentru a oferi particularului o protecție adecvată împotriva arbitrariului"; a se vedea, de asemenea, Segerstedt-Wiberg și alții v. Suedia, nr. 62332/00, 6 iunie 2006, § 76.
[257] Curtea Europeană, Weber și Saravia v. Germania (dec.), nr. 54934/00, 29 iunie 2006, § 93.
[258] Curtea Europeană, Kennedy v. Regatul Unit, citat mai sus, § 159.

societăți democratice consacrate în Convenție, ca o putere discreționară acordată executivului în domeniul securității naționale să fie exprimată în termeni de putere nelimitată[259]. Mai mult, Curtea Europeană a constatat că limitele noțiunii de securitate națională „nu pot fi extinse dincolo de sensul său natural”[260]. În consecință, legea trebuie să indice cu suficientă claritate întinderea puterii discreționare conferite autorităților competente și modalitățile de exercitare a acesteia, având în vedere scopul legitim al măsurii în cauză, de a oferi persoanei o protecție adecvată împotriva ingerințelor arbitrare.[261] Curtea Europeană a constatat că statele nu pot face afirmații generale cu privire la domeniul de aplicare al securității naționale, care ar face imposibilă contestarea efectivă a alegației de către un reclamant.[262]

82. După cum s-a observat mai sus, puține state reglementează în mod specific programe spion ca instrument de supraveghere țintită, în timp ce multe dintre ele le consideră ca un „mijloace tehnice speciale” de supraveghere fără a prevedea reguli specifice. Dacă unele regimuri juridice interne sunt destul de detaliate și precise, altele tind să se bazeze pe formulări relativ largi și deschise, care nu oferă neapărat gradul necesar de certitudine și precizie. Comisia de la Veneţia consideră că, având în vedere nivelul deosebit de ridicat de intruziune a programelor spion, în special faptul că poate implica o combinaţie de intruziuni diferite în viața privată, în cazul în care autorizează utilizarea programelor spion, statele ar trebui să adopte o legislație specifică și adaptată, cu un domeniu de aplicare *ratione personae, materiae* și *temporis* mai strict *în raport* cu alte măsuri de supraveghere țintită. Aceasta ar trebui să fie o condiție prealabilă pentru utilizarea de către stat a programelor spion.

3. *Necesitatea de a stabili o distincție între diferitele niveluri de intruziune ale supravegherii*

83. După cum s-a observat mai sus, o serie de date cu caracter personal pot fi puse la dispoziție prin supraveghere prin intermediul programelor spion care se introduc în dispozitivele electronice. Cercetările comparative au desmonstrat că, în țările care reglementează în mod specific utilizarea programelor spion, tipul de date care ar putea fi colectate diferă. Datele privind utilizarea reală a programelor spion sunt, în mod natural, rare.[263]

84. O întrebare specială apare în cazurile în care supravegherea audio sau video în direct pe un dispozitiv este activată de la distanță. Cel puțin în unele state, în afara problemei specifice a programelor spion, interceptarea în timp real a comunicațiilor (adică supravegherea audio a unei localități) este în general percepută ca fiind mai intruzivă pentru viața privată decât interceptarea conținutului telecomunicațiilor. Activarea unui telefon mobil pentru a acționa ca un dispozitiv de interceptare în timp real este chiar mai intruzivă, deoarece va urmări ținta oriunde merge și orice face. În astfel de state, pare rezonabil ca, în cazul în care se aplică limite speciale în legislație

[259] Curtea Europeană, Roman Zakharov v. Rusia [MC], citată mai sus, § 247
[260] Curtea Europeană, C.G. și alții v. Bulgaria, nr. 1365/07, 24 aprilie 2008, § 43.
[261] Curtea Europeană, Liu v. Rusia, nr. 42086/05, 6 decembrie 2007, § 56, cu trimiteri suplimentare.
[262] Curtea Europeană, Amie și alții v. Bulgaria, nr. 58149/09, 12 februarie 201, §§ 92 și 98.
[263] A se vedea, de exemplu, practica suedeză, menționată la nota de subsol 74 de mai sus, care prevede că utilizarea programelor spion în Suedia este aproape exclusiv pentru interceptarea telecomunicațiilor și colectarea datelor conținute în dispozitiv (și anume, nu pentru supravegherea audio sau video).

în ceea ce privește aplicarea legii sau utilizarea în siguranță a intercepției în timp real a comunicațiilor, de exemplu, praguri minime de gravitate în ceea ce privește infracțiunile, legături suficient de proxime, dacă nu directe, cu o amenințare reală și gravă la adresa securității naționale sau limite sau interdicții privind utilizarea interceptării în timp real a comunicațiilor în anumite locuri (locuri de cult, mass-media, birourile avocaţilor etc.) trebuie să se aplice şi atunci când poliţia sau agenţia de securitate solicită activarea funcţiei de supraveghere audio pe un telefon sau alt dispozitiv. În cazul în care legile relevante prevăd că supravegherea audio/video se limitează la locurile în care se poate presupune că suspectul se află în situație de ședere, care urmează să fie definite în mandatul de autorizare, apoi, astfel de limite trebuie să se aplice, de asemenea, atunci când programul spion este utilizat pentru a activa supravegherea audio.[264]

85. Programul spion poate prezenta o provocare specială în acest sens, deoarece din motive tehnice, nu este mereu posibilă limitarea informațiilor astfel colectate. Având în vedere caracterul extraordinar de intruziv al programului spion în comparație cu alte abordări de supraveghere, filtrarea informațiilor autorizate și neautorizate (sau relevante și irelevante) poate fi dificilă din punct de vedere tehnic. Comisia de la Veneţia îndeamnă insistent statele care iau în considerare utilizarea programelor spion să se asigure că dispun, ca garanție obligatorie, de echipe specializate, verificate și profesioniste capabile să pună în aplicare o filtrare eficientă a informațiilor, așa cum este cazul pentru alte practici de colectare a informațiilor. Cerințele în materie de distrugere ar trebui, de asemenea, să fie instituite, susținute de un control extern puternic, independent și dotat cu suficiente resurse.[265] Acest control extern trebuie să fie solid și funcțională atât în teorie, cât și în practică.

86. Revenind la întrebarea dacă este justificat să se utilizeze un program spion pentru a activa funcția de supraveghere video a unui dispozitiv mobil, Comisia de la Veneţia notează că supravegherea video în direct este, fără îndoială, una dintre cele mai intruzive funcţii pe care un program spion ar putea activa. Având în vedere caracterul său intruziv, dacă este autorizată, legislația ar trebui să prevadă un cadru strict și clar pentru activarea sa, inclusiv impunerea obligației organismului solicitant (și, la rândul său, organismului de autorizare) de a specifica tipul de informații urmărite, precum și limitele temporale și geografice ale supravegherii. De asemenea, trebuie să se aplice exigențele în materie de distrugere descrise mai sus.

87. Comisia de la Veneţia consideră că legislaţia internă trebuie să facă o distincţie clară între tipul de investigaţie în cadrul căreia poate fi autorizată utilizarea unui program spion şi datele personale ale ţintei sau ale altor persoane care pot fi căutate. Această distincție afectează evaluarea necesității și proporționalității măsurilor

[264] A se vedea, de exemplu, SOU 2023:78, citat mai sus, secțiunea 3.2.8, p. 73.

[265] De exemplu, abordarea suedeză implică stabilirea a două sau mai multe "niveluri" de acces la material în cadrul organizației de investigare. După cum s-a menționat mai sus (punctul 14), utilizarea programelor spion necesită un grup de experți specializați. Acest grup va fi invariabil separat de unitatea responsabilă cu investigarea infracțiunii specifice sau a amenințării la adresa securității naționale (ofițeri de poliție sau de informații). Comisia nu va trebui să știe (și de obicei nu va ști) nimic despre investigația reală. Grupul de experți adună echipamentul, elimină orice material care nu este acoperit de parametrii de timp și loc stabiliți în autorizație și distruge echipamentul excedentar (a se vedea punctele 126-129 de mai jos). Un astfel de sistem pe mai multe niveluri poate reduce șansele de a colecta prea multe informații. Cu toate acestea, pentru ca aceasta să funcționeze, este necesar în mod evident ca ancheta să fie o infracțiune foarte specifică sau o amenințare reală și gravă la adresa securității naționale și ca autorizația să stabilească limite temporale și spațiale clare pentru supraveghere. În plus, fiecare acces la materialul colectat trebuie înregistrat într-o manieră inviolabilă. Aceste jurnale trebuie, la rândul lor, să fie supravegheate de unul sau mai multe niveluri de revizuire/control intern, a se vedea SOU 2023:78, citat mai sus, p. 190.

întreprinse. O astfel de evaluare ar trebui să țină cont, în special, atât de durata măsurilor, cât și de intensitatea intruziunii acestora în viața privată și/sau de familie a unei persoane.[266]

B. Domeniul de aplicare *ratione personae* al măsurilor de supraveghere țintită

88. O altă exigență standard care rezultă din jurisprudența Curții Europene este aceea că legea să prevadă în mod clar că măsurile de supraveghere țintită sunt disponibile doar pentru dispozitivele de comunicare ale unei persoane care este bănuită personal de comiterea unei infracțiuni grave sau care să reprezinte o amenințare specifică la adresa securității naționale.[267]

89. Conform jurisprudenței Curții Europene, măsurile de interceptare a unei persoane care nu este bănuită de o infracțiune sau care să reprezinte o amenințare la adresa securității naționale pot, în mod excepțional, să fie justificate în temeiul articolului 8 din Convenţie.[268] Cu toate acestea, acest lucru este posibil numai dacă sunt îndeplinite anumite cerințe stricte, adică, numai dacă există motive deosebit de puternice pentru a crede că o altă persoană care este suspectă va contacta dispozitivul celeilalte persoane, sau este posibil ca coordonatele materiale să fie găsite pe dispozitivul acestei alte persoane.[269] Comisia de la Veneția consideră că, în cazul în care un stat dorește să permită, în mod excepțional, supravegherea în astfel de scopuri, atunci o astfel de posibilitate ar trebui combinată cu o autorizare prealabilă [judiciară] și și un control consolidat, de exemplu o cerință specifică de notificare a organismului de control, combinată cu o obligație procedurală a organismului de control de a acorda o atenție deosebită unor astfel de cazuri.[270] În plus, cercul terților care pot face obiectul măsurilor de interceptare ar trebui să fie specificat în decizia în cauză, iar autoritatea care acordă autorizația ar trebui să prezinte motive suficiente pentru decizia sa cu privire la acest aspect.[271]

90. Alte limite pot include doar examinarea metadatelor istorice (stocate), nu a datelor sau comunicațiilor în timp real și a activării funcțiilor de supraveghere audio sau video.[272]

91. În mod evident, apar probleme speciale atunci când o organizație face obiectul unei investigații. Acest lucru se poate întâmpla atât pentru crima organizată, cât și pentru amenințările la adresa securității naționale. Organizațiile pot fi, de asemenea, „fluide” în practică. O organizație „solidă” este o organizație care prezintă o structură

[266] Trebuie stabilite cerințe diferite în funcție de gradul de intruziune în măsura solicitată, de exemplu de gravitatea încălcării. Astfel cum s-a discutat mai sus (nota de subsol 71 și punctul 48), Codul de procedură penală olandez, astfel cum a fost modificat în 2019, prevede cinci tipuri diferite de acte de investigație care pot fi dispuse de la ofițerul de anchetă prin accesarea unui dispozitiv utilizat de un suspect – cu criterii diferite de aplicabilitate ratione materiae; în Suedia (a se vedea punctul 51 de mai sus), reglementarea face distincția între redarea de date care implică și cea care nu implică activarea microfonului unui dispozitiv pentru a înregistra sunet - cu diferite categorii de infracțiuni care justifică autorizarea măsurii.
[267] Curtea Europeană, Roman Zakharov v. Rusia [MC], supra, § 231.
[268] Curtea Europeană, Greuter v. Țările de Jos (dec.), nr. 40045/98, 19 martie 2002.
[269] Trebuie remarcat faptul că aceste rezultate au fost obținute în contextul supravegherii tradiționale și nu al măsurilor de supraveghere intruzive, pentru care ar trebui probabil utilizat un prag mai mare.
[270] În cazul Haščák v. Slovacia, nr. 58359/12, 27787/16 și 67667/16, 23 iunie 2022, § 95, Curtea Europeană a Drepturilor Omului a statuat că legea aplicabilă nu oferă nicio protecție persoanelor afectate aleatoriu de măsurile secrete de supraveghere.
[271] Curtea Europeană, Pietrzak și Bychawska-Siniarska și alții v. Polonia, citată anterior, § 201.
[272] A se vedea, de exemplu, legislația suedeză (a se vedea punctul 51 de mai sus) care impune astfel de limite în secțiunea 5.

și componență fixă a personalului, în timp ce o organizație „fluidă” este mai informală în ceea ce privește componența și timpul. Trebuie să se acorde o atenţie deosebită formulării condiţiilor de utilizare a programelor spion în astfel de circumstanţe, pentru a nu submina garanţiile acordate persoanelor.[273] Datorită naturii mai vagi a securităţii naţionale şi a potenţialului său mai mare de abuz, aceste garanţii sunt deosebit de importante în acest caz.

92. Trebuie notat faptul că unele state interzic utilizarea supravegherii țintite prin intermediul programelor spion pe calculatoare sau telefoanele unui avocat, ale unui jurnalist sau ale unui medic.[274] În cazul în care acest lucru este permis, în mod excepțional, Curtea Europeană și Comisia de la Veneția au concluzionat anterior că, în cazul în care supravegherea ar fi efectuată împotriva jurnaliștilor și a avocaților, trebuie să se aplice standarde mai înalte pe parcursul acestor operațiuni (praguri mai ridicate înainte de aprobarea operațiunilor de supraveghere, control intern și extern mai exigent etc.)[275]

1. Utilizarea programelor spion împotriva jurnaliștilor și a altor actori media

93. Îndeosebi cu referire la jurnalism, este bine stabilit faptul că instrumentele de supraveghere pot fi aplicate numai în cele mai excepționale circumstanțe. Surse europene și internaționale au recunoscut pe scară largă că rolul de câine de gardă al jurnalismului necesită o precauție excepțională atunci când se analizează interferențele cu funcțiile lor. Curtea Europeană a menţionat că „autorităţile au doar o marjă limitată de apreciere pentru a decide dacă există o „necesitate socială imperioasă”” pentru a satisface necesitatea unei ingerinţe în viața privată și în libertatea de exprimare a jurnaliștilor.[276] Protecția se extinde la organizațiile neguvernamentale care cercetează și diseminează informații în interes public[277] precum și cadre universitare, scriitori, bloggeri și alte persoane pe internet.[278] Experţii internaţionali au cerut „măsuri cuprinzătoare” pentru a proteja jurnaliştii de supraveghere.[279] Consiliul Europei a considerat de mult timp că ordinele sau acțiunile de interceptare, supravegherea și alte forme de căutare sau ridicare a datelor jurnalistice „nu ar trebui să fie aplicate în cazul în care scopul lor este de a eluda dreptul jurnaliștilor [.] de a nu dezvălui informații care identifică sursele lor”.[280]

94. Aceste principii au o pondere deosebită în contextul programelor spion, în special deoarece, după cum a remarcat Autoritatea Europeană pentru Protecția

[273] A se vedea de exemplu recomandările formulate de CTIVD olandez în Raportul de revizuire 53 privind utilizarea competenței de investigare în materie de piraterie de către AIVD și MIVD în 2015, 8 martie 2017, p. 17.
[274] A se vedea secțiunea IV.B de mai sus.
[275] Comisia de la Veneția, CDL-AD(2015)011, citată mai sus § 103; în ceea ce privește jurnaliștii, a se vedea Curtea Europeană, Telegraaf Media Nederland Landelijke Media B.V. și alții v. Țările de Jos, nr. 39315/06, 22 noiembrie 2012; în ceea ce privește avocații, a se vedea Bersheda și Rybolovlev v. Monaco, nr. 36559/19 și 36570/19, 6 iunie 2024, §§ 73-76. În ceea ce privește jurnaliștii și mass-media în special, a se vedea și legislația UE privind libertatea mass-mediei, citată mai sus.
[276] Curtea Europeană, Stoll v. Elveția [MC], nr. 69698/01, 10 decembrie 2007, § 105.
[277] Curtea Europeană, Animal Defenders International v. Regatul Unit, nr. 48876/08, 22 aprilie 2013, §103.
[278] Curtea Europeană, Magyar Helsinki Bizottság v. Ungaria, nr. 18030/11, 8 noiembrie 2016, § 168.
[279] A se vedea, de exemplu, Declarația comună privind libertatea și democrația mass-mediei, Raportorul special al Organizației Națiunilor Unite (ONU) pentru promovarea și protecția dreptului la libertatea de opinie și de exprimare, Reprezentantul Organizației pentru Securitate și Cooperare în Europa (OSCE) pentru libertatea mass-mediei, Raportorul special al Organizației Statelor Americane (OAS) pentru libertatea de exprimare și Raportorul special al Comisiei Africane de Exprimare. Drepturile omului și ale popoarelor (CADHP) privind libertatea de exprimare și accesul la informații în Africa, 2 mai 2023.
[280] Consiliul Europei, Recomandarea nr. R (2000) 7 a Comitetului de Miniștri către statele membre privind dreptul jurnaliștilor de a nu dezvălui sursele lor de informare, Anexă: Principiul 6, 8 martie 2000.

Datelor, „Pegasus nu ar trebui să fie echivalat cu instrumentele de interceptare „tradiționale" a forțelor de ordine".[281] Comisarul pentru Drepturile Omului al Consiliului Europei, evaluând dificultatea extremă de limitare a accesului programelor spion în anumite cazuri, a remarcat că, chiar și în contextul unui cadru de garanții, „este practic de neimaginat că utilizarea Pegasus sau a unui program spion echivalent ar putea fi considerată vreodată conformă cu legea și cu garanțiile necesare definite de Curte".[282] Înaltul Comisar ONU pentru Drepturile Omului a avertizat în mod special că „efectele paralizante" ale programului spion asupra jurnalismului ar putea duce la „erodarea guvernanței democratice".[283]

95. Legislația europeană privind libertatea presei a Uniunii Europene, care a intrat în vigoare în 2024 și se va aplica din august 2025, a încercat să ssoluționeze această problemă. Articolul 4 § 3 (c) din Act prevede, ca regulă generală, că programele spion nu pot fi utilizate împotriva furnizorilor de servicii media sau a altor persoane care ar putea duce la divulgarea surselor și comunicațiilor. Acesta prevede derogări de la această protecție standard numai în cazul în care: (i) autoritățile demonstrează existența unui motiv imperativ de interes public; (ii) există o autorizare *ex ante* din partea unei autorități judiciare sau a unei autorități decizionale independente și imparțiale sau, în cazuri excepționale și urgente, este autorizată ulterior de o astfel de autoritate; (iii) ancheta se referă la infracțiuni deosebit de grave și implică o persoană vizată;[284] (iv) nicio altă măsură mai puțin restrictivă nu ar fi adecvată și suficientă pentru obținerea informațiilor solicitate.

96. Puterile extrem de intruzive oferite de programele spion amenință produsul muncii jurnaliștilor și disponibilitatea surselor de a vorbi cu ei. Scandalul Pegasus a arătat că jurnaliștii erau aparent vizați doar pentru că sunt jurnaliști, ceea ce este inacceptabil într-o societate democratică. Comisia de la Veneția consideră că legislația ar trebui să definească strict țintele posibile ale măsurilor de supraveghere și să prevadă că anumite categorii de persoane ale căror interacțiuni pot fi protejate de privilegiul profesional, precum și jurnaliștii, sunt în principiu excluse, cu anumite excepții limitate. În cazul în care se pretinde, din motive justificate, că aceste persoane comit o infracțiune specifică, definită și gravă și reprezintă o amenințare specifică definită la adresa securității naționale și că, prin urmare, este necesară o anchetă judiciară, Comisia de la Veneția consideră, în conformitate cu jurisprudența CEDO, că trebuie aplicate standarde puternic îmbunătățite, inclusiv praguri mai ridicate înainte de aprobarea operațiunilor de supraveghere și un control intern și extern mai exigent (a se vedea paragraful 92 de mai sus).

C. Domeniul de aplicare *ratione materiae* al măsurilor de supraveghere țintită

[281] Autoritatea Europeană pentru Protecția Datelor, Observații preliminare privind programele spion moderne, 15 februarie 2022.
[282] Programele spion extrem de intruzive amenință însăși esența drepturilor omului, citat mai sus.
[283] Dreptul la viața privată în era digitală, supra.
[284] Articolul 4 alineatul (3) litera (c) din această legislație se referă la aceste persoane ca fiind „furnizorii de servicii mass-media, redacția acestora sau orice persoană care, în temeiul relației lor obișnuite sau profesionale cu un furnizor de servicii mass-media sau cu echipa sa editorială, poate deține informații referitoare la surse sau comunicări jurnalistice confidențiale sau la identificarea acestora".

97. De asemenea, este important ca legislația să stabilească în mod clar natura infracțiunilor care pot da naștere unui ordin de interceptare. Astfel cum s-a menționat anterior, condițiile de claritate și previzibilitate a legii nu impun statelor să stabilească exhaustiv infracțiunile specifice care pot da naștere la interceptare. Cu toate acestea, ar trebui furnizate suficiente detalii privind natura infracțiunilor în cauză.[285] În timp ce statele au, în principiu, autoritatea suverană de a determina ce este și ce nu este o infracțiune gravă în conformitate cu legislația națională, CEDO a arătat clar că acesta este un subset mai mic al întregului grup de infracțiuni: un stat nu este liber să extindă această categorie, astfel încât să acopere în practică majoritatea infracțiunilor.[286] Acest lucru este valabil a fortiori pentru măsurile de supraveghere intruzivă.[287]

98. Cu referire la amenințările la adresa securității naționale, după cum s-a ilustrat mai sus, cerința de „previzibilitate" a legii nu merge atât de departe încât să oblige statele să adopte dispoziții legale care să enumere în detaliu toate comportamentele care pot determina o decizie de a supune o persoană supravegherii secrete din motive de „securitate națională". Cu toate acestea, domeniul de aplicare al oricărei puteri discreționare conferite autorităților competente trebuie să fie strict definit, în special în ceea ce privește domeniul de aplicare material și personal al autorizației [judiciare] prealabile (a se vedea concluziile CEDO de la paragraful 81 de mai sus). În plus, așa cum s-a menționat deja, un control eficient devine și mai important. CJUE a elaborat standarde specifice în ceea ce privește securitatea națională, susținând, în special, că statele membre, atunci când iau măsuri pentru a proteja securitatea națională, trebuie să poată demonstra că există motive suficient de solide pentru a crede că se confruntă cu o amenințare gravă la adresa securității naționale, care este stabilită ca fiind reală și prezentă sau previzibilă[288]; trebuie să demonstreze că este necesar să recurgă la o derogare de la dreptul UE pentru a proteja securitatea națională[289] și că necesitatea de a proteja securitatea națională nu ar fi putut fi satisfăcută prin aplicarea dispozițiilor relevante ale dreptului UE[290].

D. Limitele temporale ale măsurilor de supraveghere țintită

99. Problema duratei totale a măsurilor de supraveghere direcționată poate fi lăsată la latitudinea autorităților responsabile de emiterea și reînnoirea mandatelor de interceptare, cu condiția să existe garanții adecvate, cum ar fi indicarea clară în dreptul intern a perioadei după care un mandat de interceptare expiră, a condițiilor în care un mandat poate fi reînnoit și a circumstanțelor în care acesta trebuie revocat[291]. Curtea Europeană a Drepturilor Omului a criticat legislația națională pentru că nu a prevăzut

[285] Curtea Europeană, Kennedy v. Regatul Unit, citat anterior, § 159.
[286] Curtea Europeană, Iordachi și alții v. Moldova, nr. 25198/02, 10 februarie 2009, § 44..
[287] De exemplu, legislația UE privind libertatea mass-mediei prevede că software-ul de supraveghere intruzivă trebuie să fie utilizat asupra profesioniștilor din domeniul mass-mediei numai dacă este utilizat în contextul investigațiilor privind infracțiunile enumerate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI a Consiliului, pedepsite în statul membru în cauză cu o pedeapsă privată de libertate sau cu o măsură de siguranță cu o durată maximă de cel puțin trei ani, sau în contextul anchetelor privind alte infracțiuni grave pedepsite în statul membru în cauză cu o pedeapsă privată de libertate sau o măsură de siguranță cu o durată maximă de cel puțin cinci ani, astfel cum este stabilită de dreptul intern al statului membru respectiv, și cu condiția ca nicio altă măsură mai puțin restrictivă să nu fie adecvată și suficientă pentru a obține informațiile urmărite.
[288] CJUE, La Quadrature du Net, citată mai sus, § 137
[289] A se vedea, mutatis mutandis, CJUE, Comisia Europeană/ Republica Polonă și alții, cauzele conexate C-715/17, C-718/17 și C-719/17, §§152 și 159
[290] A se vedea, mutatis mutandis, CJUE, Comisia Europeană/ Republica Austria (denumită în continuare "Tipografia de Stat"), cauza C-187/16, §§ 78-80.
[291] Curtea Europeană, Roman Zakharov v. Rusia [MC], supra, § 250.

un termen clar pentru autorizarea unei măsuri de supraveghere direcționată[292]. CJUE a susținut că, atunci când un stat membru adoptă o măsură legislativă care prevede colectarea în timp real a datelor de trafic și de localizare care vizează o persoană, aceasta trebuie să fie limitată în timp la ceea ce este „strict necesar”.[293] Comisia de la Veneția consideră că, cu cât o ingerință în viața privată durează mai mult, cu atât mai mari sunt efectele sale asupra drepturilor și libertăților omului, ceea ce necesită o justificare mai puternică. Perioadele mai lungi vor fi mai dificil de justificat în temeiul principiilor necesității și proporționalității.

100. Pe lângă chestiunea duratei, Comisia de la Veneția consideră că, în acest context, este necesar să se țină cont și de gradul de intruziune în viața privată al unei măsuri de supraveghere. Cu cât o măsură este mai intruzivă, cu atât perioadele de autorizare ar trebui să fie mai scurte. În toate cazurile în care se autorizează o perioadă lungă de supraveghere sau în care o perioadă scurtă trebuie reînnoită (în mod frecvent și repetat), este deosebit de important să se impună organismului de anchetă obligația de a informa imediat instanța sau organismul de autorizare și/sau organismul de control în cazul în care condițiile se schimbă în cursul anchetei. Într-adevăr, este posibil ca o investigație demarată cu bună credință cu privire la o infracțiune gravă pentru care este autorizată supravegherea intruzivă să se transforme, în timp, într-o investigație cu privire la o infracțiune mai puțin gravă pentru care nu este autorizată supravegherea intruzivă - caz în care cea mai intruzivă formă de supraveghere ar trebui oprită imediat.

101. Limitele de timp pot fi aplicate și în alt sens, și anume clauze de caducitate, care precizează că legislația privind supravegherea va expira după un anumit număr de ani (a se vedea, de exemplu, nota de subsol 243 de mai sus). Această dispoziție poate fi combinată cu cerința de a efectua o anchetă oficială privind modul în care a fost utilizată legislația și de a face publică această anchetă (cel puțin în măsura în care este posibil). Aceasta este o bună practică și sperăm că va servi la asigurarea publicului că puterile nu sunt utilizate în mod abuziv.

E. Testul celei mai mici intruziuni posibile

102. În ceea ce privește condițiile care trebuie consacrate în lege, o cerință standard pentru toate metodele speciale de investigare este impunerea unui test al „mijloacelor cele mai puțin intruzive” - acesta este un corolar natural al principiului proporționalității. Curtea Europeană a Drepturilor Omului a clarificat acest lucru în contextul interceptării în masă[294], dar se aplică mutatis mutandis măsurilor de supraveghere țintită. Organul solicitant trebuie să demonstreze organului de autorizare că informațiile căutate în cadrul investigației nu pot fi obținute prin mijloace mai puțin intruzive. În acest sens, ar trebui evaluate posibilele efecte pozitive ale unei prelucrări speciale și specifice a datelor, de preferință printr-o combinație de surse independente de probe și practici comparative.

[292] Curtea Europeană, Iordachi și alții v. Moldova, citată mai sus, § 45
[293] CJUE, La Quadrature du Net, citat anterior, § 189.
[294] Curtea Europeană, Big Brother Watch și alții v. Regatul Unit [MC], citat mai sus, § 448.

103. Procedura de autorizare și controlul ar trebui să fie riguroase pentru a evita ca astfel de cerințe să devină mai degrabă simple formalități decât cerințe juridice substanțiale care trebuie îndeplinite în mod clar. Aceasta nu este doar o chestiune de securitate juridică. Întrucât utilizarea programelor spion tinde să fie un proces care implică foarte multe resurse, serviciile de poliție sau de securitate responsabile de anchetă ar trebui să aibă, de asemenea, un interes puternic în guvernarea eficientă a resurselor lor.[295]

F. Autorizarea și controlul măsurilor de supraveghere țintită de către un organism judiciar sau de către un alt organism independent

104. În conformitate cu jurisprudența Curții Europene, controlul și supravegherea măsurilor de supraveghere secretă pot interveni la trei stadii: atunci când supravegherea este dispusă pentru prima dată, în timp ce se desfășoară sau după încetarea acesteia. În ceea ce privește primele două etape, însăși natura și logica supravegherii secrete impune ca nu numai supravegherea în sine, ci și controlul care o însoțește să fie efectuate fără cunoștința persoanei. Astfel, întrucât persoanele vor fi în mod necesar împiedicate să exercite un remediu efectiv din proprie inițiativă sau să participe direct la orice procedură de reexaminare, este esențial ca procedurile stabilite să ofere garanții adecvate care să le protejeze drepturile. Într-un domeniu în care abuzul de putere este eventual atât de ușor și ar putea avea consecințe nefaste pentru o societate democratică în ansamblu, Curtea a statuat că, în principiu, este de dorit să se încredințeze controlul de supraveghere unui judecător, controlul judiciar oferind cele mai bune garanții de independență, imparțialitate și o procedură adecvată.[296]

105. O procedură de autorizare pur politică, adică în care poliția sau o agenție de securitate solicită autorizarea din partea ministrului responsabil, nu este acceptabilă în temeiul CEDO[297] și a PIDCP. Cu toate acestea, este posibil să se combine cele două proceduri, autorizarea fiind solicitată unui ministru al guvernului (care s-ar concentra probabil pe problema capacității), în timp ce chestiunea legalității este stabilită de instanță. După cum a stabilit Curtea Europeană în mod repetat, începând cu cauza *Klass*, este preferabilă autorizarea judiciară, deoarece ea oferă cele mai bune garanții de independență, imparțialitate și o procedură adecvată.[298] Cu toate acestea, în anumite domenii pot exista motive pentru a înlocui o instanță cu un organism de autorizare expert, cu condiția ca acest organism să îndeplinească standarde înalte de independență. Comisia de la Veneția consideră, în conformitate cu practica Curții Europene, că existența unui organism de autorizare expert poate fi mai justificată în ceea ce privește supravegherea în masă,[299] însă autorizația judiciară

[295] Instrumente de investigație pentru dispozitivele Poliției Regale Canadiene (RCMP) și chestiuni conexe, supra, la p. 21
[296] Curtea Europeană, Roman Zakharov v. Rusia [MC], supra, § 233.
[297] Curtea Europeană, Big Brother Watch și alții v. Regatul Unit [MC], citat mai sus, § 351. A se vedea, de asemenea, o hotărâre publicată recent (numai în malteză) a Primei Curți a Curții Civile din Malta (acționând în calitate de Curtea Constituțională), care a statuat că dreptul la un proces echitabil al unui reclamant al cărui telefon a fost interceptat a fost încălcat deoarece interceptările au fost efectuate în temeiul unui mandat emis de executiv și nu de o autoritate judiciară.
[298] A se vedea Curtea Europeană, Klass și alții v. Germania, nr. 5029/71, 6 septembrie 1978, §§ 55-56, și Roman Zakharov v. Rusia [MC], citat anterior, § 233.
[299] A se vedea Comisia de la Veneția, CDL-AD(2015)010, citată mai sus, §§ 210, 250; CDL-AD(2015)011, citat mai sus, §§ 24, 115-122; a se vedea, de asemenea, Curtea Europeană, Big Brother Watch și alții împotriva Hotărârii Europene a Drepturilor Omului, Hotărârea Big Brother Watch și alții împotriva Hotărârii T Regatul Unit [GC], citat mai sus, § 351, citând hotărârea camerei Big Brother Watch și alții v. Regatul Unit, nr. 58170/13, 62322/14, 24960/15, 13 septembrie 2018, §§ 318-320

trebuie preferată în cadrul supravegherii direcționate. Acest lucru nu exclude un grad de specializare a instanței sau a instanțelor care pot autoriza utilizarea programelor spion (a se vedea paragraful 111 de mai jos).

106. În contextul supravegherii secrete, Curtea Europeană a constatat că, în cazuri excepționale de urgență, este posibil ca măsura de supraveghere vizată să fie efectuată fără autorizare prealabilă, cu condiția ca instanța sau organismul independent relevant să o autorizeze într-un termen scurt.[300] Recent, CtEDO a constatat că o perioadă de cinci zile pentru ca o instanță să acorde sau să respingă *a posteriori* cererea de măsură de supraveghere specifică nu a oferit suficiente garanții, deoarece aplicarea procedurii de autorizare de urgență a fost justificată numai de riscul de pierdere a probelor și nu de gravitatea sau natura infracțiunii. Curtea a constatat că, având în vedere pericolele pe care le implică recurgerea la o astfel de procedură de urgență nejudiciară pentru sfera privată a persoanei care face obiectul supravegherii secrete, legislația aplicabilă ar trebui să conțină suficiente garanții pentru a se asigura că utilizarea sa este rezonabilă și limitată la cazuri justificate în mod corespunzător, inclusiv garanții împotriva utilizării repetate a măsurii în cauză.[301]

1. *Criterii de evaluare de către instanța de autorizare/organismul independent*

107. Curtea Europeană a subliniat că instanța de autorizare/instanța de autorizare/organismul independent trebuie să poată evalua caracterul rezonabil al utilizării măsurii în cazul particular și a constatat încălcări ale CEDO în cazurile în care nu a existat nicio indicație că judecătorii care au emis mandatele au îndeplinit o funcție de control.[302]

108. În această privință, Curtea Europeană examinează, de asemenea, domeniul de aplicare al controlului (dacă judecătorul aplică un test de „necesitate” sau „proporționalitate”) și conținutul autorizației de interceptare. Este o practică obișnuită să se solicite organului de anchetă să furnizeze instanței sau organului de autorizare independent baza pentru autorizare, exprimată de obicei ca indicii „concrete” sau „faptice” (de un anumit nivel) ale unei infracțiuni în curs sau iminente sau ale unei amenințări la adresa securității naționale, precum și un anumit prag probatoriu.

109. Supravegherea țintită este uneori autorizată nu numai pentru investigarea infracțiunilor sau a amenințărilor la adresa securității naționale din trecut sau prezent (în curs), ci și a infracțiunilor potențiale, viitoare sau a amenințărilor la adresa securității naționale. Comisia de la Veneția consideră că, în general, legislația ar trebui să prevadă standarde materiale mai ridicate și praguri de probă atunci când vine vorba de autorizarea utilizării programului spion pentru a investiga în mod iminent/infracțiuni sau amenințări viitoare (de exemplu, în ceea ce privește indicațiile concrete). Autorizarea judiciară sau independentă care nu examinează aceste aspecte esențiale nu reprezintă o garanție reală. Toate aceste cerințe pentru a furniza indicații concrete/faptice și pentru a respecta anumite praguri probatorii trebuie să fie însoțite de obligația autorității solicitante de a documenta acest lucru în cerere. Acest lucru

[300] Curtea Europeană, Ekimdzhiev și alții v. Bulgaria, Nr. 70078/12, 11 ianuarie 2022, §323.
[301] Curtea Europeană, Pietrzak și Bychawska-Siniarska și alții v. Polonia, citată mai sus, § 208.
[302] Curtea Europeană, Ekimdzhiev și alții v. Bulgaria, citată mai sus, §§307-322; Haščák v. Slovacia, citată mai sus; Zoltán Varga împotriva Slovaciei, citată mai sus.

este necesar, în parte deoarece condițiile s-ar putea schimba în cursul anchetei și în parte pentru că va fi necesar pentru supravegherea ulterioară care trebuie să aibă loc.

110. În sfârșit, autoritatea solicitantă ar trebui să examineze în permanență persistența motivelor supravegherii și să informeze organismul de autorizare atunci când și dacă motivele aplicării măsurii se modifică. În cazul în care aceste motive nu se mai aplică, supravegherea trebuie întreruptă imediat.[303]

2. *Specializarea organelor judiciare și a altor organisme independente*

111. Unele state au prevăzut un anumit grad de specializare, de exemplu în ceea ce privește procurorii și/sau instanțele judecătorești sau, după cum s-a menționat mai sus, în crearea unor organisme specializate independente de autorizare pentru supravegherea specifică. De asemenea, pot fi prevăzute niveluri diferite de autorizare care să corespundă diferitelor tipuri de investigații/date solicitate sau în ceea ce privește modul în care se efectuează supravegherea, fizic sau de la distanță.[304] După cum s-a menționat deja (nota de subsol 266), există, de asemenea, unități specializate în unele agenții de aplicare a legii. Astfel de unități oferă suportul tehnic necesar pentru implementarea programului de supraveghere intruzivă, dar și sprijină unitățile operaționale în îndeplinirea cerințelor legale necesare pentru utilizarea unui astfel de software. Pot exista avantaje pentru eficiență și supraveghere în concentrarea competențelor către un anumit organism specializat în aplicarea legii sau securitate/inteligență. În plus, după cum s-a menționat, aceasta poate contribui la menținerea confidențialității în ceea ce privește gestionarea informațiilor obținute în raport cu alte părți ale organizației de investigare). În orice caz, trebuie să existe norme și să fie respectate cu strictețe, limitând informațiile care pot fi stocate, analizate și comunicate altor părți ale agenției de investigare sau în afara agenției. [305]

112. După cum a menționat anterior Comisia de la Veneția, un anumit grad de specializare poate avea avantaje, deoarece, prin repetarea frecventă, cei implicați în procesul de autorizare devin mai experți în materie. Astfel, un organism mai expert ar putea fi mai înclinat să stabilească condiții mai multe și mai bune pentru autorizațiile pe care le emite. În același timp, este important să se evite „înăsprirea cazurilor” (o tendință a judecătorilor specializați de a se identifica cu cei responsabili de securitate) și să se mențină încrederea publicului în integritatea sistemului de autorizare.[306]

3. *Apărători ai vieții private și ai securității*

113. Comisia de la Veneția a observat anterior că faptul că autorizarea măsurilor de supraveghere se realizează fără știrea persoanei poate fi compensat, într-o anumită

[303] A se vedea, de exemplu, în Republica Slovacă, articolele 4 § 6 și 6 § 1 din PAIA.
[304] În Țările de Jos, Consiliul Procurorilor Generali (direcția națională a Parchetului) autorizează utilizarea programelor spion în anchetele penale. În Elveția, pentru măsurile de informații desfășurate pe teritoriul Federației, măsura de informații trebuie să fie autorizată de președintele unei secții speciale a Curții Administrative Federale. În plus, măsura trebuie aprobată de ministrul apărării după consultarea ministrului afacerilor externe și a ministrului justiției; Consiliul Federal (guvernul elvețian) poate fi sesizat cu privire la cazuri de importanță deosebită. În Spania, un judecător al Curții Supreme (al camerei administrative sau penale) și un adjunct sunt numiți pentru a autoriza interceptarea comunicațiilor de către serviciile de informații. În Suedia, articolul 14 din Legea (2020:62) privind citirea datelor secrete prevede că, în cazuri specifice legate de suspecții străini de terorism, este competentă o instanță specializată (Tribunalul Districtual din Stockholm).
[305] Curtea Europeană, Centrul pentru Justiție cv. Suedia [MC], citat anterior, § 276.
[306] Comisia de la Veneția, CDL-AD(2015)010, citată mai sus, §§ 221-223.

măsură, prin prezența, în cadrul procedurii de autorizare, a apărătorilor vieții private, adică a profesioniștilor din domeniul juridic care reprezintă interesele persoanelor și organizațiilor vizate în cadrul procedurii de autorizare.[307] Faptul că astfel de avocați pot oferi o garanție reală în cadrul procedurilor depinde de o serie de factori. Procurorul (sau organismul solicitant) va fi, în general, în posesia unui număr mult mai mare de probe. Un avocat supus controlului de securitate nu acționează direct pentru suspect și, evident, nu îl poate consulta pe acesta. Avocatul poate avea foarte puțin timp la dispoziție pentru a se familiariza cu cazul și, prin urmare, poate fi dezavantajat procedural în comparație cu procurorul. În Suedia, o comisie de anchetă a constatat că obligația de a implica un avocat care a făcut obiectul unei anchete de securitate a dus rareori, dacă nu chiar niciodată, la un refuz de autorizare.[308] Pe de altă parte, mecanismul poate avea încă o anumită valoare prin faptul că poate duce la impunerea unor condiții pentru a reduce la minimum intruziunea în viața privată, pentru ținta sau alte persoane afectate de supraveghere. În plus, aceasta poate formaliza procesul de obținere a autorizației, făcând mai clar faptul că organismul solicitant are sarcina de a demonstra necesitatea utilizării supravegherii, și că toate condițiile de supraveghere sunt îndeplinite.

G. Sistemele naționale de control

114. Controlul este esențial pentru a contribui la asigurarea faptului că programele spion - care cauzează interferențe atât de semnificative cu dreptul la viață privată și la protecția datelor - sunt utilizate în conformitate cu legea. Controlul este, de asemenea, necesar pentru a preveni abuzurile poliției și ale serviciilor de informații și pentru a se asigura că aceste servicii își îndeplinesc mandatele și își utilizează competențele și resursele în mod adecvat și eficient.

115. Comisia de la Veneția a subliniat, în contextul controlului agențiilor de securitate, că principala garanție împotriva abuzurilor de putere este controlul intern de către serviciile de securitate însele, pentru a se asigura că personalul care lucrează în cadrul agențiilor este angajat față de valorile democratice ale statului și față de respectarea drepturilor omului.[309] Un aspect similar poate fi formulat în ceea ce privește aplicarea legii.

116. Cu toate acestea, un control extern este, de asemenea, necesar pentru a asigura parlamentul și publicul că procedurile de control intern sunt respectate în mod corespunzător.[310] Deși, în principiu, este de dorit ca controlul autorizațiilor să fie încredințat unei instanțe judecătorești, controlul post-hoc efectuat de organisme nejudiciare poate fi considerat compatibil cu CEDO, cu condiția ca organismul de control să fie independent de autoritățile de control și să fie învestit cu suficiente puteri și competențe pentru a exercita un control efectiv și continuu[311] și pentru a asigura o protecție efectivă împotriva abuzurilor, inclusiv competențe de investigare și reparație. Mandatele organismelor de supraveghere se completează reciproc, astfel încât, luate în ansamblu, acestea să asigure o supraveghere continuă și garanții adecvate.

[307] Comisia de la Veneția, CDL-AD(2015)011, citată mai sus, § 100; CDL-AD(2016)012, citată mai sus, § 97.
[308] Vezi ancheta oficială suedeză privind supravegherea secretă, SOU 2012:44.
[309] Comisia de la Veneția, CDL-AD(2015)010, § 134.
[310] A se vedea și articolul 11 § 3 din Convenția 108+.
[311] Curtea Europeană, Roman Zakharov v. Rusia [MC], citată mai sus, § 275.

Această complementaritate poate fi realizată prin cooperare informală între organismele de supraveghere sau prin mijloace legale[312]. În contextul „interceptării în masă", CEDO a subliniat necesitatea unor garanții „de la un capăt la altul", care să acopere întregul proces de supraveghere, inclusiv problema transferului de informații/material către alte organizații decât cea care efectuează ancheta, în propriul stat și în alte state.[313]

117. Există o diferență între controlul de securitate/al informațiilor și controlul poliției/al aplicării legii. Operațiunile de supraveghere a aplicării legii tind să ajungă în urmărire penală și, prin urmare, există, în cele din urmă, o oportunitate pentru controlul judiciar post-hoc. Acest lucru tinde să nu se întâmple în cazul activităților de securitate/informații și, prin urmare, trebuie instituite organisme specializate de control/supraveghere. După cum s-a arătat mai sus, existența comitetelor parlamentare de supraveghere este o caracteristică comună a sistemului de supraveghere a securității/informațiilor în statele membre.[314] Parlamentele se bucură de legitimitate democratică și pot trage la răspundere executivul pentru modul în care acesta conduce și supraveghează activitățile serviciilor de securitate.[315] Acestea fiind spuse, Comisia de la Veneția a avertizat anterior împotriva deficiențelor supravegherii pur parlamentare. [316] Organismele de experți, care efectuează supravegherea activităților serviciilor de informații într-un număr de state, s-au dovedit a fi mai reușite și mai eficiente în mai multe state, sau, de asemenea, o combinație între un organism specializat și un organism parlamentar.[317]

118. În cazul în care un stat nu a înființat un organism specializat de supraveghere a securității, Autoritățile de Protecție a Datelor (APD) pot juca un rol important în sistemul de supraveghere a securității și a informațiilor în ansamblu, în special în ceea ce privește dosarele de securitate (deși trebuie remarcat faptul că multe APD nu au competența de a investiga chestiuni de securitate națională).[318] Furnizarea de către instituțiile independente de supraveghere a unor competențe suficiente și de resurse umane (inclusiv profesioniști calificați din punct de vedere tehnic și specializați), financiare și tehnice este esențială, în special având în vedere competențele și capacitățile extinse pe care serviciile de informații le au în general și natura secretă a multora dintre activitățile lor. Pe lângă discutarea rapoartelor anuale, a anchetelor și a auditurilor periodice, APD-urile ar trebui să poată iniția investigații la scară largă, precum și investigații ad-hoc și să aibă acces permanent, complet și direct la informații clasificate, și documente pentru îndeplinirea eficientă a mandatului lor.

119. Comisia de la Veneția împărtășește punctul de vedere al Agenției pentru Drepturi Fundamentale a UE, potrivit căruia organismele care exercită supravegherea serviciilor de informații ar trebui să evolueze într-un mod similar cu legile și capacitățile serviciilor de informații. Competențele și competențele mai mari ale acestora din urmă trebuie să fie echilibrate printr-un grad mai mare de supraveghere independentă,

[312] Raport al FRA, secțiunea 1.2, opinia 6.
[313] A se vedea, de exemplu, Curtea Europeană, Big Brother Watch v. Regatul Unit [MC], citat mai sus, § 350; Centrum för Rättvisa v. Suedia [MC], citată mai sus.
[314] A se vedea secțiunea IV.E de mai sus și raportul FRA, citat mai sus, § 1.5.2.
[315] Controlul democratic și efectiv al serviciilor naționale de securitate, citat mai sus, p. 45.
[316] În contextul supravegherii strategice, a se vedea Comisia de la Veneția, CDL-AD(2015)011, citată mai sus, §§ 108-109.
[317] Comisia de la Veneția, CDL-AD(2015)010, citată mai sus, §§ 228-250.
[318] Report de la FRA, secțiunea 2.3.

împreună cu resurse și expertiză adecvate pentru a asigura o supraveghere eficientă.[319] Cooperarea dintre autoritățile de supraveghere relevante ar trebui să asigure supravegherea „de la început până la sfârșit" garantată de CEDO.[320] Este important să se adopte o abordare holistică în ceea ce privește problema supravegherii și ca competențele de control prevăzute de lege să fie implementate în practică.

H. Notificarea măsurilor de supraveghere țintită

120. Curtea Europeană solicită ca persoana plasată sub supraveghere să fie în mod normal informată ulterior, astfel încât să poată fi implicată în controlul măsurii. Astfel, aceasta a stabilit o obligație generală de notificare retroactivă, sub rezerva unor excepții.[321] În cazul în care nu există un mecanism permanent de reclamații, apoi, absența totală a unei cerințe de notificare a subiectului interceptării la un moment dat după încetarea supravegherii a fost considerată incompatibilă cu Convenția, prin faptul că privează subiectul interceptării de posibilitatea de a solicita reparații pentru ingerințe ilegale în drepturile sale prevăzute la articolul 8 și face ca căile de atac să fie disponibile în temeiul dreptului național mai degrabă teoretice și iluzorii decât practic și eficient.[322] În schimb, Curtea a constatat că absența oricărei obligații de notificare a persoanei în cauză cu privire la măsura de interceptare în orice etapă a aplicării sale a fost compatibilă cu Convenția, în cazul în care persoanele care au suspectat că comunicările lor au făcut sau au făcut obiectul unei interceptări ar putea sesiza un organism independent de soluționare a plângerilor, cu competențe depline de investigare, și a căror jurisdicție nu a făcut obiectul notificării interceptării.[323] Deși este posibil să nu se poată solicita notificarea în toate cazurile, este de dorit să se notifice persoana vizată de supraveghere de îndată ce notificarea poate fi făcută fără a pune în pericol scopul măsurilor și după ridicarea măsurilor de supraveghere.[324] Într-o hotărâre recentă, bazându-se, printre altele, pe constatările unui aviz anterior al Comisiei de la Veneția, CEDO a constatat că absența unei obligații de notificare în contextul polonez al supravegherii secrete, chiar și după o anumită perioadă de timp, a fost unul dintre elementele care au condus la concluzia că cadrul juridic general a fost în încălcare a articolului 8 din Convenție.[325]

121. După cum s-a menționat mai sus, notificarea unei ținte individuale poate compromite în mod evident metodele confidențiale sau operațiunile în curs. Cu toate acestea, este important să se prevadă o obligație generală pentru autoritățile competente de a notifica ținta ex post și de a formula excepții de la această regulă. Decizia de a nu notifica o țintă într-un anumit caz, chiar și după încheierea supravegherii, trebuie să fie întotdeauna notificată organismului de control extern și, în mod normal, aprobată de acesta. În cazul în care notificarea a fost făcută, iar

[319] Raportul FRA, secțiunea 1.2, opinia 3.
[320] Curtea Europeană, Segerstedt-Wiberg și alții v. Suedia, citată mai sus; a se vedea, de asemenea, raportul FRA, secțiunea 3. De asemenea, trebuie remarcat faptul că articolul 17 din Convenția 108+ impune cooperarea obligatorie a autorităților de supraveghere în cazurile transfrontaliere.
[321] Curtea Europeană, Roman Zakharov v. Rusia [MC], citată mai sus, §§ 286 și următoarele.
[322] Curtea Europeană, Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdzhiev v. Bulgaria, nr. 62540/00, 28 iunie 2007, §§ 90-91.
[323] Curtea Europeană, Kennedy v. Regatul Unit, citată mai sus, § 167.
[324] Curtea Europeană, Pietrzak și Bychawska-Siniarska și alții v. Polonia, citată mai sus, § 238.
[325] Ibidem, §§ 238-247; a se vedea Comisia de la Veneția, CDL-AD(2016)012, citată mai sus. Cerințe similare au fost impuse de Curtea de Justiție a Uniunii Europene în cauzele Tele2 și Watson și Quadrature du Net, citate mai sus.

persoana este, prin urmare, conștientă de supraveghere, procedura ex parte în fața instanței care a emis mandatul de supraveghere poate fi completată de o procedură complet contradictorie în cursul căreia instanța va examina de novo legalitatea supravegherii. Notificarea este, în primul rând, un mecanism de obținere a unei reparații. Comisia de la Veneția a considerat că este necesar ca persoanele care pretind că au fost prejudiciate de competențele excepționale ale agențiilor de securitate și de informații să dispună de o cale de atac.[326]

122. Articolul 13 din CEDO impune statelor să instituie un mecanism efectiv de remediere pentru pretinsele încălcări ale drepturilor din Convenție. De asemenea, articolul 12 din Convenția 108+ impune sancțiuni și remedii judiciare și nonjudiciare adecvate pentru încălcarea dispozițiilor Convenției.[327]

123. Agenția pentru Drepturi Fundamentale a Uniunii Europene a subliniat necesitatea de a asigura cerințe minime pentru ca măsurile corective să fie eficiente:[328] în primul rând, organismele extrajudiciare trebuie să fie independente; în plus, acestea trebuie: (i) să sensibilizeze persoanele cu privire la măsurile de supraveghere, fie prin notificare, fie prin orice altă posibilitate de a obține informații cu privire la interceptări; (ii) să asigure accesul la informații clasificate pentru organismele de remediere; (iii) să asigure căile de atac adecvate, de exemplu, distrugerea datelor colectate sau scutirea monetară; și (iv) asigurarea unei expertize adecvate în cadrul organismelor de remediere.

I. Protecția terților împotriva măsurilor legate de utilizarea programelor spion

124. Una dintre particularitățile utilizării programelor spion este că, în funcție de circumstanțe, aceasta poate fi efectuată de la distanță (executarea codului de la distanță) sau fizic (deși acest lucru este probabil mai rar, deoarece este necesar ca poliția sau agenția de securitate să fi obținut temporar acces la dispozitivul unui suspect). Executarea codului de la distanță este unică prin faptul că exploatarea unei vulnerabilități care permite accesul poliției sau agenției de securitate la dispozitivul suspectului poate exacerba vulnerabilitățile software și hardware ale dispozitivelor terților.[329] Aici trebuie găsit un echilibru dificil. Pe de o parte, poliția/agenția de securitate poate avea motive întemeiate pentru a păstra tăcerea cu privire la o anumită vulnerabilitate, pe care au găsit-o sau creat-o, deoarece acest lucru le va permite să exploateze acest lucru în scopuri de investigație în viitor. Pe de altă parte, lăsarea acestor vulnerabilități deschise înseamnă că actorii rău intenționați, cum ar fi membrii grupurilor de crimă organizată etc., le pot găsi și exploata. Prin urmare, legislația ar

[326] Pentru o prezentare generală a concluziilor Comisiei de la Veneția privind mecanismele de depunere a plângerilor, a se vedea Comisia de la Veneția, CDL-AD(2015)010, citată mai sus, §§ 251 și următoarele.
[327] În ceea ce privește autoritățile de protecție a datelor, raportul FRA, citat mai sus, secțiunea 2.3, oferă o imagine de ansamblu a competențelor de remediere ale autorităților de protecție a datelor din Europa.
[328] Raportul FRA, secțiunea 2.1.
[329] Autoritatea italiană pentru protecția datelor a evidențiat riscurile la adresa vieții private în cazul în care inocularea unui instrument de supraveghere intruziv nu este directă, ci se face prin descărcarea de aplicații de pe platforme accesibile gratuit oricărui utilizator. În acest caz, există un risc de instalare de către terți care nu au nicio legătură cu obiectivele anchetei. Prin urmare, acest risc ar trebui eliminat permițând utilizarea numai a aplicațiilor care împiedică achiziția de către terți sau prevăzând că activitatea de captură ar trebui să înceapă numai după verificarea faptului că programul este asociat în mod unic cu dispozitivul corespunzător celei reglementată de decretul de autorizare, a se vedea documentul aprobat de Comisia a 2-a permanentă (Justiție) în cadrul reuniunii sale din 20 septembrie 2023 la încheierea anchetei de constatare a faptelor pe tema interceptărilor convorbirilor telefonice, citat anterior, p. 43.

trebui să prevadă protecția părților terțe împotriva exploatării vulnerabilităților de programe informatice de către agențiile de aplicare a legii sau de informații. În plus, agențiile de aplicare a legii sau de informații nu ar trebui să lase securitatea programului sau a materialului afectat într-o stare în general mai proastă decât înainte de începerea operațiunii.

125. Într-un stat s-a sugerat ca poliţia/agenţia de securitate să stabilească un mecanism care să cântărească corect avantajele şi dezavantajele păstrării tăcerii /dezvăluirii în fiecare caz și documentarea procesului său decizional în această privință (permițând un control viitor și, dacă este necesar, o obligație de raportare). În plus, s-a sugerat să se prevadă un registru central al vulnerabilităților pentru fiecare agenție.[330]

J. Obligația de a distruge „informații excedentare”

126. După cum sa menționat deja, utilizarea programelor spion permite măsuri precum monitorizarea în timp real a comunicațiilor, mișcărilor sau activităților online, căutarea datelor stocate pe dispozitiv și activarea unei camere și a unui microfon încorporate pentru supraveghere. Utilizarea programului spion împotriva unui dispozitiv mobil poate duce astfel la colectarea de „informații excedentare”, adică informații care nu sunt pertinente pentru investigația/supravegherea specială pentru care a fost acordată autorizația. O astfel de colectare prezintă riscuri deosebit de grave pentru viața privată și alte drepturi fundamentale ale țintei și ale persoanelor aflate în contactele sale și ridică întrebări serioase cu privire la proporționalitatea oricărei utilizări a programelor spion.

127. Curtea Europeană a subliniat în mod constant necesitatea unei cerințe de a distruge imediat orice date care nu sunt relevante pentru scopul pentru care au fost obținute.[331] Este deosebit de important să existe astfel de dispoziții în ceea ce privește utilizarea programelor spion din cauza multitudinii diferitelor tipuri de informații, unele dintre ele fiind informații cu caracter personal deosebit de sensibile, care poate rezulta din această activitate.[332]

128. Două tipuri diferite de informații pot rezulta dintr-o investigație/supraveghere care nu au făcut parte din justificarea eliberării autorizației de utilizare a programelor spion. Primul este reprezentat de informații cu caracter personal care nu privesc o infracțiune sau o amenințare la adresa securității naționale. Aceste informații ar trebui să facă obiectul unei cerințe de distrugere imediată.[333] Acest lucru ar trebui să fie susținut de supraveghere.[334] Al doilea tip de informații este reprezentat de informații

[330] Raportul de revizuire 53 privind utilizarea competenței de investigare în legătură cu pirateria de către AIVD și MIVD în 2015, citat mai sus, p. 25.
[331] Curtea Europeană, Roman Zakharov v. Rusia [MC], citată mai sus, § 255, referindu-se la Klass și alții v. Germania, citată anterior, § 52.
[332] Curtea Constituțională a Republicii Moldova, în decizia nr. 31 din 23 septembrie 2021, a considerat că este necesar ca apărarea să aibă posibilitatea de a accesa, fie la finalul urmăririi penale, fie la finalul procesului pe fond, meta-datele obținute ca urmare a aplicării supravegherii secrete, chiar și atunci când distrugerea informațiilor obținute prin supravegherea secretă a meta-datelor a fost dispusă deoarece a fost considerată irelevantă de către judecătorul de instrucție.
[333] A se vedea, de exemplu, secțiunea 23 din Legea suedeză (2020:62) privind citirea datelor secrete.
[334] Desigur, poate fi dificil să reconciliezi cerințele de control și distrugere, deoarece dacă acestea din urmă funcționează corect, organismul de control nu are nimic de „monitorizat”. Cu toate acestea, este posibil să se documenteze faptul că informațiile au fost distruse și data la care au avut loc. În plus, organismul de control poate verifica dacă cerințele existente privind distrugerea automată funcționează, de exemplu testându-le cu informații ipotetice.

care indică faptul că există o amenințare diferită la adresa securității naționale,[335] sau infracţiunea, a avut loc sau se produce sau va avea loc în curând, adică diferită de cea pentru care a fost acordată autorizaţia.

129. Pentru a evita utilizarea abuzivă a programelor spion și pentru a menține încrederea publicului că sistemul nu este abuzat, o regulă rezonabilă este de obicei să solicite distrugerea acestor informații. Se poate prevedea o excepție în cazul în care infracțiunea sau amenințarea la adresa securității naționale în cauză, fără a face parte din baza autorizației inițiale, este, cu toate acestea, este suficient de grav (o ameninţare reală şi gravă), dacă s-ar cunoaşte la momentul respectiv, pentru a îndeplini condiţiile de autorizare a utilizării programului spion în primul rând.[336] Permiterea unei astfel de excepții presupune o anumită formă de acces stratificat la materialul colectat (a se vedea nota de subsol 266 de mai sus). În plus, pentru a preveni ca această excepție să devină, în practică, regula, ar trebui să existe cerința de a solicita și de a obține permisiunea de a păstra astfel de informații strict definite de către instanța (sau organismul independent) care a autorizat în primul rând mandatul inițial. Toate aceste acordări de permisiune ar trebui, de asemenea, să fie documentate și urmate de o supraveghere externă.

K. Controlul exportului programelor spion

130. După cum s-a arătat mai sus, în conformitate cu Rezoluția APCE 2513(2023), unele state membre ale Consiliului Europei ar fi putut, de asemenea, să exporte Pegasus sau programe spion similare către țări terțe cu regimuri opresive și autoritare. În Rezoluția 2045(2015), APCE a îndemnat statele membre și cele cu statut de observator să se abțină, printre altele, de la exportul de tehnologie avansată de supraveghere către regimurile autoritare.[337] O problemă conexă este aceea că programele spion comerciale sunt dezvoltate de companii private. După cum au arătat dezvăluirile Pegasus, companiile private au fost implicate nu numai în producția de programe spion, ci și în furnizarea de programe spion ca serviciu. În acest sens, externalizarea funcțiilor „de bază” ale statului, cum ar fi supravegherea, către companii dornice să își vândă serviciile și să obțină profit, în special într-un sector privat nereglementat, comportă riscuri foarte mari de utilizare abuzivă a acestor tehnologii, pe lângă riscul asociat cu lipsa de responsabilitate.[338]

131. Programele spion sunt considerate tehnologii cu dublă utilizare (adică pot fi utilizate atât în scopuri civile, cât și militare), de unde și necesitatea de a obține o licență de export. O bună gestionare a industriei programelor spion necesită un control eficient al exporturilor. Regulamentul (UE) 2021/821 a instituit un regim de control al exporturilor, al intermedierii, al asistenței tehnice, al tranzitului și al transferului de produse cu dublă utilizare (Regulamentul privind produsele cu dublă utilizare).[339] În Acordul de la Wassenaar au fost stabilite norme globale, la care 31 de state membre

[335] Acest lucru presupune în mod evident că amenințările la adresa securității naționale pot fi specificate cu suficientă precizie.
[336] A se vedea, de exemplu, articolele 28-31 din Legea suedeză (2020:62) privind citirea datelor secrete.
[337] APCE, Rezoluția 2045 (2015), Operațiuni de supraveghere în masă, 21 aprilie 2015, punctul 19.
[338] A se vedea, mutatis mutandis, Comisia de la Veneția, CDL-AD(2009)038, Raport privind companiile militare și de securitate private și erodarea monopolului de stat asupra utilizării forței.
[339] Regulamentul (UE) 2021/821 al Parlamentului European și al Consiliului din 20 mai 2021 de instituire a unui regim al Uniunii pentru controlul exporturilor, intermediere, asistență tehnică, tranzit și transfer de produse cu dublă utilizare (reformare).

ale Consiliului Europei sunt părți.[340] Acordul de la Wassenaar a fost încheiat în 1999 ca un acord multilateral de control al exporturilor între state pentru a contribui la securitatea și stabilitatea regională și internațională, promovează transparența și o mai mare responsabilitate în ceea ce privește transferurile de arme convenționale și de produse și tehnologii cu dublă utilizare. Cu toate acestea, acordul nu conține orientări sau măsuri de aplicare care să abordeze în mod direct încălcările drepturilor omului cauzate de instrumentele de supraveghere.[341]

132. Comisia de la Veneția consideră că statele participante la Acordul de la Wassenaar ar putea explora posibilitatea condiționării normelor privind acordarea licențelor tehnologice în ceea ce privește respectarea de către statul primitor (și de către societatea producătoare) a standardelor privind drepturile omului.[342] În ceea ce privește societățile private, acordarea de licențe de export ar putea fi condiționată de punerea în aplicare a Principiilor directoare ale Organizației Națiunilor Unite privind afacerile și drepturile omului în ceea ce privește proiectarea, vânzarea și, transferul sau sprijinirea acestor tehnologii. [343] Acest lucru este în conformitate cu recomandările relevante făcute de PACE [344] și de Parlamentul European [345] De asemenea, urmează linia adoptată în prezent de statele care participă la Declarația Comună privind Eforturile de Combatere a Proliferării și a Utilizării abuzive a programului spion comercial (a se vedea nota de subsol 252 de mai sus). Angajamentele asumate ar putea fi dezvoltate în continuare, urmând recomandările-cheie cuprinse în raportul Raportorului special al ONU pe 2019 privind promovarea și protecția dreptului la libertatea de opinie și expresia este, printre altele: (i) să instituie un moratoriu imediat privind vânzarea și transferul global de tehnologie de supraveghere privată până la instituirea unor garanții riguroase în materie de drepturi ale omului pentru a reglementa astfel de practici și pentru a garanta că guvernele și actorii non-statali utilizează instrumentele în moduri legitime;[346] și (ii) să pună în aplicare garanții solide pentru a se asigura că orice utilizare a produselor sau serviciilor lor respectă standardele privind drepturile omului. Aceste garanții includ clauze contractuale care interzic personalizarea, țintirea, întreținerea sau orice altă utilizare care încalcă legislația internațională privind drepturile omului, caracteristici tehnice de proiectare pentru a semnala, preveni sau atenua utilizarea abuzivă, precum și audituri și procese de verificare a drepturilor omului.[347]

[340] Acordul de la Wassenaar privind controlul exporturilor de arme convenționale și de bunuri și tehnologii cu dublă utilizare. Statele participante la Aranjamentul de la Wassenaar sunt Argentina, Australia, Austria, Belgia, Bulgaria, Canada, Croația, Danemarca, Estonia, Finlanda, Franța, Germania, Grecia, Ungaria, India, Irlanda, Italia, Japonia, Letonia, Lituania, Luxemburg, Malta, Mexic, Țările de Jos, Noua Zeelandă, Norvegia, Polonia, Africa de Sud, Spania, Portugalia, Republica Coreea, Republica Cehă, România, Federația Rusă, Slovacia, Slovenia, Suedia, Elveția, Turcia, Ucraina, Regatul Unit și Statele Unite ale Americii.
[341] Raportul din 2019 al SR al Organizației Națiunilor Unite, citat mai sus, §§ 34-35.
[342] După cum sugerează Privacy International, acordarea unei licențe ar putea fi refuzată atunci când există un „risc substanțial ca astfel de exporturi să fie utilizate pentru a încălca drepturile omului, atunci când nu există un cadru legal într-o destinație care să reglementeze utilizarea unui element de supraveghere sau când cadrul legal pentru utilizarea acestuia nu este în conformitate cu legislația sau standardele internaționale privind drepturile omului”. a se vedea D. Kaye, The Spyware State and the prospects for accountability, The Global Forum, Global Governance 27 (2021) Brill Nijhoff, pp. 487-488.
[343] Organizația Națiunilor Unite, Reprezentantul Special al Secretarului General pentru problema drepturilor omului și a corporațiilor transnaționale și a altor întreprinderi, Principiile directoare privind afacerile și drepturile omului: punerea în aplicare a cadrului "Protecție, respect și remediere" al Organizației Națiunilor Unite. A se vedea, de asemenea, Ministerul pentru Afaceri Externe, Commonwealth și Dezvoltare al Regatului Unit, The Pall Mall Process: Tackling the proliferation and Irresponsible use of commercial cyber intrusion capabilities, în special punctul 8.
[344] APCE, Rezoluția 2513 (2023), citată mai sus, § 14.9.
[345] Recomandarea PE, citată mai sus, § 56.
[346] Raportul din 2019 al SR al ONU, supra, § 66 (a).
[347] Ibidem, § 67 (b).

133. În conformitate cu angajamentul multi-guvernamental menționat la paragrafele 73 și 132 de mai sus și pentru a promova transparența și controlul eficient, Comisia de la Veneția consideră, de asemenea, că guvernele ar trebui, ca o chestiune de bună practică, să facă declarații publice anuale care să indice dacă au achiziționat licențe pentru programe spion de la furnizori comerciali și, dacă da, de la care entitate comercială.[348] De asemenea, acestea ar trebui să ia în considerare orice alte măsuri de transparență adecvate, cum ar fi publicarea de rapoarte periodice privind utilizarea programelor spion și amenințările reprezentate de programele spion comerciale străine.

VI. Concluzii

134. Printr-o scrisoare din 6 decembrie 2023, Președintele de atunci al Adunării Parlamentare a Consiliului Europei (APCE), dl Tiny Kox, i-a solicitat Comisiei de la Veneția, în conformitate cu Rezoluția 2513 (2023) a Adunării Parlamentare privind „programul Pegasus și programe spion similare și supravegherea secretă a statului", să efectueze un studiu privind cadrul legislativ și practica privind supravegherea specifică a tuturor statelor membre (în mod prioritar Polonia, Ungaria, Grecia, Spania și Azerbaidjan; apoi Germania, Belgia, Luxemburg, țările de Jos și toate celelalte state membre). Ca răspuns la cerere, Comisia de la Veneția a efectuat un studiu comparativ pentru a evalua normele existente privind supravegherea specifică și, în special, privind utilizarea programelor spion în statele sale membre. Comisia de la Veneţia a luat în considerare prevederile legale ale statelor care au trimis informaţii oficiale APCE şi ale celor asupra cărora membrii Comisiei de la Veneţia/experții au furnizat informații răspunzând la un chestionar elaborat de raportori. Complexitatea cadrelor legislative în cauză, lipsa unor informații cuprinzătoare și practice privind punerea în aplicare a standardelor internaționale existente, cum ar fi articolul 9 din Convenția 108, pe lângă reglementarea specifică limitată a programelor spion, acesta a fost un factor important de luat în considerare la pregătirea raportului.

135. Programul spion este un instrument de supraveghere intruzivă care poate fi utilizat pentru a interfera cu dispozitive electronice, inclusiv smartphone-uri sau computere, fără știrea utilizatorului, permițând operatorului să pătrundă în dispozitive și, în funcție de instrumentul specific, să urmărească geo-localizarea în timp real, să citească toate datele stocate, toate comunicațiile efectuate (ocolind posibilele protecții, cum ar fi criptarea) și să preia controlul asupra tuturor dispozitivelor materiale și programelor disponibile pe dispozitiv, cum ar fi microfoanele sau camerele. Dacă nu este reglementat, programul spion s-ar putea transforma într-un dispozitiv de supraveghere 24 de ore din 24, cu acces deplin la toți senzorii și informațiile de pe dispozitivul personal. Acest lucru l-ar transforma într-o armă de supraveghere care ar putea fi utilizată pentru a restricționa drepturile omului, a cenzura și a incrimina critica și disidența și a hărțui (sau chiar a suprima) jurnaliștii, activiștii pentru drepturile omului, oponenții politici sau a suprima organizațiile societății civile, după cum au arătat numeroase acuzații și dezvăluiri. Prin urmare, este esențial să se definească în

[348] Articole de presă recente despre litigiile din Statele Unite sugerează că guvernele ar putea fi dependente de operatorii comerciali pentru a efectua supravegherea folosind programele spion.

mod clar domeniul de aplicare al utilizării programelor spion de către guverne pentru a preveni și eradica practicile abuzive.

136. Pe baza jurisprudenței Curții Europene privind supravegherea țintită, a rapoartelor anterioare ale Comisiei de la Veneția, a altor standarde europene și internaționale, cum ar fi Convenția 108+, și a unei analize comparative a legislației relevante din statele membre ale Comisiei de la Veneția, prezentul raport a încercat să identifice garanțiile minime care ar trebui instituite, în cazul măsurilor de supraveghere țintită intruzivă, pentru a evita orice abuz de putere. În cele din urmă, va reveni Curții Europene a Drepturilor Omului să stabilească standardele specifice aplicabile în acest domeniu, atunci când se va pronunța cu privire la cazurile „programelor spion" care sunt în prezent pendinte sau care i-ar putea fi prezentate.

137. Comisia de la Veneția consideră că utilizarea și dezvoltarea de programe de supraveghere intruzive, cum ar fi programele spion, ar trebui să fie posibile numai dacă cadrul juridic relevant îndeplinește anumite cerințe stricte. Cel puțin următoarele garanții trebuie implementate:

- Toate dispozițiile semnificative care reglementează utilizarea unui instrument de supraveghere intruzivă, cum ar fi programele spion (dacă există), trebuie să fie prevăzute în legislația primară, care ar trebui să definească în mod clar domeniul de aplicare (restricționat) *ratione materiae, personae* şi *temporis* de supraveghere ţintită prin programe spion, care nu pot fi asemănate cu alte măsuri de supraveghere țintită;
- În special, legislația ar trebui să definească strict țintele posibile ale măsurilor de supraveghere și să prevadă că anumite categorii de persoane ale căror interacțiuni pot fi protejate de privilegiul profesional, precum și jurnaliștii, sunt în principiu excluse, cu anumite excepții limitate;
- Legislația internă trebuie să facă o distincție clară între tipul de anchetă/supraveghere în contextul căreia poate fi autorizată utilizarea programelor spion și datele cu caracter personal care pot fi solicitate; o astfel de distincție ar trebui să influențeze evaluarea necesității și proporționalității măsurilor luate;
- Autoritățile solicitante (aplicarea legii sau agenția de informații) ar trebui să demonstreze întotdeauna că informațiile solicitate în cadrul anchetei au fost necesare în scopul legitim și nu au putut fi obținute prin mijloace mai puțin intruzive;
- Trebuie să existe proceduri de autorizare ex-ante bine reglementate în fața unei instanțe sau a unui alt organism independent (sau, în cazuri excepționale și urgente, norme care să prevadă confirmarea rapidă de către o astfel de instanță sau organism independent a măsurii de supraveghere țintite); iar durata măsurilor de supraveghere trebuie să fie limitată la strictul necesar;
- Întregul proces de supraveghere trebuie să fie susținut de instituții externe de supraveghere independente eficace, care dispun de resurse suficiente, sunt calificate și specializate și nu pot fi încredințate exclusiv executivului;
- Agenția care efectuează investigația/supravegherea autorizată și accesează datele nu trebuie să acceseze mai multe date decât este permis de autorizația primită: orice date care nu sunt relevante pentru scopul pentru care au fost

obținute ar trebui să fie identificate fără întârzieri (nejustificate) și distruse definitiv;

- Persoanele aflate în supraveghere trebuie notificate ulterior, sub rezerva excepțiilor definite de lege, astfel încât să poată fi implicate în controlul și contestarea măsurii; pentru cazurile în care acest lucru nu este posibil (de exemplu. probleme de securitate națională) în legislație trebuie introduse căile de atac;
- Legislația ar trebui să prevadă protecția terților împotriva exploatării, de către agențiile de aplicare a legii sau de informații, a vulnerabilităților programelor;
- Statele ar trebui să condiționeze normele privind acordarea licențelor pentru exportul de tehnologie de respectarea de către statul de destinație (și de către societatea producătoare) a standardelor privind drepturile omului identificate în prezentul raport;
- Guvernele ar trebui să facă declarații publice anuale în care să precizeze dacă au obținut licențe pentru programe spion de la furnizori comerciali și, în caz afirmativ, de la ce entitate comercială. De asemenea, acestea ar trebui să ia în considerare orice alte măsuri de transparență adecvate, cum ar fi publicarea de rapoarte periodice privind utilizarea programelor spion și amenințările reprezentate de programele spion comerciale străine.

138. Comisia de la Veneţia rămâne la dispoziţia Adunării Parlamentare pentru asistenţă suplimentară în acest domeniu.