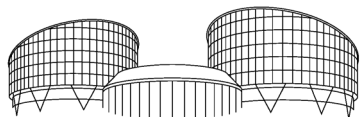


- © [Institutul European din România](#) – Această traducere nu obligă Curtea.
© European Institute of Romania - This translation does not bind the Court.
© Institut européen de Roumanie - Cette traduction ne lie pas la Cour.



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Press Unit
Unité de la Presse

Fișă tematică – Supraveghere în masă

Septembrie 2022

Această fișă tematică nu obligă Curtea și nu este exhaustivă

Supraveghere în masă

Art. 8 (dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței) din [Convenția europeană a drepturilor omului](#) prevede că:

„1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.

2. Nu este admis amestecul unei autorități publice în exercitarea acestui drept decât în măsura în care acest amestec este prevăzut de lege și dacă constituie o măsură care, într-o societate democratică, este necesară pentru securitatea națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirea faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora”.

Pentru a stabili dacă ingerința autorităților în viața privată sau corespondența reclamanților era necesară într-o societate democratică și a fost păstrat un just echilibru între diferitele interese implicate, Curtea Europeană a Drepturilor Omului examinează dacă ingerința era prevăzută de lege, urmărea un obiectiv legitim sau obiective legitime și dacă era proporțională cu obiectivul urmărit.

[Klass și alții împotriva Germaniei](#)

6 septembrie 1978 (hotărâre)

În această cauză, reclamanții, cinci avocați germani, se plâneau, în special, de legislația din Germania care autoriza autoritățile să le monitorizeze corespondența și comunicațiile telefonice fără a obliga autoritățile să-i informeze ulterior despre măsurile luate împotriva lor.

Curtea Europeană a Drepturilor Omului a hotărât că **nu a fost încălcat art. 8** din Convenția Europeană a Drepturilor Omului, constatând că legiuitorul german era justificat să considere ingerința rezultată din legislația contestată în exercitarea dreptului garantat de art. 8 ca fiind necesară într-o societate democratică în interesul securității naționale și pentru a preveni dezordinea sau faptele penale. Curtea a observat, în special, că aceste competențe de a supraveghea în secret cetățenii, caracteristice unui stat polițienesc, sunt tolerabile în temeiul Convenției numai în măsura strict necesară pentru protejarea instituțiilor democratice. Constatând, însă, că, în prezent, societățile democratice sunt amenințate de forme extrem de sofisticate de spionaj și de terorism, ceea ce impune ca statul să fie capabil în mod efectiv, pentru a contracara efectiv astfel de amenințări, să supravegheze în secret elementele subversive care operează în jurisdicția sa, Curtea a considerat că existența unei anumite legislații care acordă competența de a supraveghea în secret corespondența, comunicările prin poștă și telecomunicațiile era, în condiții excepționale, necesară într-o societate democratică, în interesul securității naționale și/sau pentru a preveni dezordinea sau faptele penale.

[Weber și Saravia împotriva Germaniei](#)

29 iunie 2006 (decizie privind admisibilitatea)

Reclamanții – primul, un jurnalist independent, al doilea prelua mesajele telefonice pentru primul reclamant și i le transmitea – au susținut, în special, că anumite dispoziții din Legea din 1994 privind combaterea infracționalității, care modifica Legea din 1968 privind

limitarea secretului corespondenței, poștei și telecomunicațiilor („Legea G 10”)¹, astfel cum au fost interpretate și modificate de Curtea Constituțională Federală prin hotărârea din 14 iulie 1999, le încălca dreptul la respectarea vieții private și a corespondenței.

Curtea a declarat plângerea reclamantilor **inadmisibilă** ca fiind vădit nefondată. Având în vedere toate dispozițiile contestate din Legea G 10, astfel cum a fost modificată, în contextul legislativ existent, Curtea a constatat că existau garanții adecvate și efective împotriva abuzurilor privind competențele de monitorizare strategică ale statului. În consecință, Curtea a fost convinsă că Germania, în cadrul marjei sale de apreciere destul de largi în acest domeniu, era îndreptățită să considere că ingerințele în secretul telecomunicațiilor rezultate din dispozițiile contestate au fost necesare într-o societate democratică, în interesul securității naționale și pentru a preveni săvârșirea de infracțiuni.

Liberty si alții împotriva Regatului Unit

1 iulie 2008 (hotărâre)

Reclamantele, o organizație britanică și două organizații irlandeze pentru protecția libertăților civile, au susținut că, între 1990 și 1997, telefoanele, faxurile, mesageriile electronice și comunicațiile de date, inclusiv informații confidențiale și supuse secretului profesional, au fost interceptate de un dispozitiv de testare electronic gestionat de Ministerul Apărării britanic. Au introdus cereri în fața Tribunalului pentru Litigii referitoare la Interceptarea Comunicațiilor (Interception of Communications Tribunal), a Procurorului General (Director of Public Prosecutions) și a Tribunalului pentru Litigii referitoare la Competențele de Investigare (Investigatory Powers Tribunal) pentru a contesta legalitatea interceptării comunicațiilor acestora, însă fără niciun rezultat.

Curtea a hotărât că, în speță, **a fost încălcat art. 8** din Convenție. A considerat că, la momentul relevant, dreptul intern nu indica cu suficientă claritate, astfel încât să ofere o protecție adecvată împotriva abuzului de putere, domeniul de aplicare sau modul de exercitare a marjei de apreciere foarte extinse conferite autorităților pentru a intercepta și examina comunicațiile externe. În special, nu prevedea, astfel cum impune jurisprudența Curții, într-o formă accesibilă publicului, nicio indicație despre procedura aplicabilă selectării în vederea examinării, partajării, stocării și distrugerii materialului interceptat. Ingerința în drepturile reclamantelor în temeiul art. 8 nu era, prin urmare, „prevăzută de lege”.

Kennedy împotriva Regatului Unit

18 mai 2010 (hotărâre)

Suspectând că poliția îi intercepta comunicațiile după ce a început o mică afacere, reclamantul a formulat o plângere către Tribunalul pentru Litigii referitoare la Competențele de Investigare [Investigatory Powers Tribunal (IPT)]. În cele din urmă, a fost informat, în 2005, că nu s-a constatat nimic în favoarea sa în privința plângerilor formulate. Aceasta însemna că comunicațiile sale nu au fost interceptate sau că IPT a considerat toate interceptările ca fiind legale. IPT nu a furnizat informații suplimentare. Reclamantul se plângea despre presupusa interceptare a comunicațiilor sale.

Curtea a hotărât că **nu a fost încălcat art. 8** din Convenție, constatând că legislația Regatului Unit privind interceptarea comunicațiilor interne, coroborată cu clarificările aduse prin publicarea unui cod de deontologie, indica cu o claritate suficientă procedurile de autorizare și prelucrare a mandatelor de interceptare, precum și prelucrarea, comunicarea și distrugerea datelor colectate. În plus, nu exista nicio dovadă a unor deficiențe semnificative în aplicarea și funcționarea regimului de supraveghere. Prin urmare, având în vedere garanțiile împotriva abuzurilor, precum și garanțiile mai generale

¹. Legea G 10 a fost modificată pentru a soluționa așa-numita monitorizare strategică a telecomunicațiilor, respectiv colectarea de informații prin interceptarea telecomunicațiilor pentru a identifica și a preveni pericolele grave cu care se confrunta Republica Federală Germania, ca de exemplu un atac armat pe teritoriul său sau comiterea de atacuri teroriste internaționale și alte infracțiuni grave. Modificările vizau, în special, extinderea puterilor Serviciului de Informații Federal în privința înregistrării telecomunicațiilor în cursul unei monitorizări strategice, precum și utilizarea datelor cu caracter personal obținute prin intermediul acestora și transmiterea lor către alte autorități.

oferite de controlul Comisarului și examinarea efectuată de IPT, măsurile de supraveghere contestate, în măsura în care ar fi putut să fie aplicate reclamantului, erau justificate în temeiul art. 8 din Convenție.

Roman Zaharov împotriva Rusiei

21 februarie 2013 (hotărâre – Marea Cameră)

Această cauză privea sistemul de interceptare secretă a comunicațiilor de telefonie mobilă în Rusia. Reclamantul, editor-șef al unei edituri, se plângea, în special, de faptul că operatorii de rețele de telefonie mobilă din Rusia erau obligați prin lege să instaleze echipamente care să permită agențiilor de aplicare a legii să desfășoare măsuri operative de investigații și că, fără garanții suficiente în temeiul dreptului rus, acest fapt permitea interceptarea generalizată a comunicațiilor.

Curtea a hotărât că **a fost încălcat art. 8** din Convenție, constatând că dispozițiile legale ruse care reglementau interceptarea comunicațiilor nu ofereau garanții adecvate și efective împotriva arbitrarului și riscurilor de abuz inerente oricărui sistem de supraveghere secretă, care era extrem de ridicat într-un sistem precum cel din Rusia, în care serviciile secrete și poliția aveau acces direct, prin mijloace tehnice, la toate comunicațiile de telefonie mobilă. În special, Curtea a constatat deficiențe în ceea ce privește cadrul legal în următoarele domenii: circumstanțele în care autoritățile publice din Rusia sunt abilitate să recurgă la măsuri de supraveghere secretă; durata unor astfel de măsuri, în special circumstanțele în care ar trebui să înceteze; procedurile de autorizare a interceptării, precum și stocarea și distrugerea datelor interceptate; controlul interceptărilor. În plus, caracterul efectiv al căilor de atac disponibile pentru a contesta interceptarea comunicațiilor era afectat de faptul că acestea erau disponibile numai persoanelor care puteau să probeze interceptarea și că obținerea unor astfel de probe era imposibilă în lipsa unui sistem de notificare sau a posibilității de a avea acces la informații privind interceptarea.

A se vedea, de asemenea, în ceea ce privește măsurile secrete de supraveghere în contextul procedurilor penale: **Ahliustin împotriva Rusiei**, **Zubkov și alții împotriva Rusiei**, **Moskalev împotriva Rusiei** și **Konstantin Moskalev împotriva Rusiei**, hotărâri din 7 noiembrie 2017.

Szabó și Vissy împotriva Ungariei

12 ianuarie 2016 (hotărâre)

Această cauză privea legislația ungară referitoare la supravegherea secretă antiteroristă, introdusă în 2011. Reclamantii se plângeau, în special, că exista posibilitatea de a face obiectul unor măsuri nejustificate și disproporționat intruzive, în cadrul juridic ungar, de supraveghere secretă în scopuri legate de securitatea națională [și anume „art. 7/E (3) privind supravegherea”]. Susțineau, în special, că acest cadru juridic era predispus la abuzuri, în special în lipsa unui control jurisdicțional.

Curtea a hotărât că, în speță, **a fost încălcat art. 8** din Convenție. A admis că era o consecință firească a formelor actuale ale terorismului ca guvernele să recurgă la tehnologii de vârf, inclusiv la o monitorizare masivă a comunicațiilor, pentru a anticipa incidente iminente. Cu toate acestea, Curtea nu a fost convinsă că legislația în cauză oferea suficiente garanții pentru evitarea abuzurilor. În special, domeniul de aplicare al măsurilor putea include practic orice persoană în Ungaria, date fiind noile tehnologii care permit Guvernului să intercepteze volume mari de date chiar și despre persoane din afara sferei inițiale a operațiunii. Pe de altă parte, dispunerea unor astfel de măsuri s-a luat în întregime de către organul executiv și fără a exista o evaluare dacă interceptarea comunicațiilor era strict necesară și fără ca măsuri corective efective, nici măcar judiciare, să fie puse în aplicare. Curtea a hotărât, în continuare, că în speță **nu a fost încălcat art. 13** (dreptul la un recurs efectiv) din Convenție, **coroborat cu art. 8**, reiterând faptul că art. 13 nu poate fi interpretat ca impunând o cale de atac împotriva stadiului în care se află dreptul intern.

Breyer împotriva Germaniei

30 ianuarie 2020 (hotărâre)

În conformitate cu modificările aduse în 2004 Legii privind telecomunicațiile din Germania, companiile trebuiau să colecteze și să stocheze datele cu caracter personal ale tuturor clienților acestora, inclusiv ale utilizatorilor de cartele SIM preplătite, ceea ce nu se solicitase anterior. Reclamanții, activiști ai libertății civile și critici ai supravegherii statului, erau utilizatori ai unor astfel de cartele și prin urmare au fost obligați să își înregistreze date personale precum numerele de telefon, data nașterii, precum și numele și adresa lor, la prestatorii de servicii. Aceștia se plâneau de stocarea datelor lor cu caracter personal ca utilizatori de cartele preplătite.

Curtea a hotărât că **nu a fost încălcat art. 8** din Convenție, constatând că, în general, Germania nu și-a depășit limitele puterii sale discreționare („marja de apreciere”) pe care o avea în aplicarea legii în cauză, atunci când a ales mijloacele de atingere a scopurilor legitime de protejare a securității naționale și de combatere a infracționalității, și că stocarea datelor cu caracter personal ale reclamanților fusese proporțională și „necesară într-o societate democratică”. Prin urmare, nu a existat nicio încălcare a Convenției. Curtea a considerat, în special, că colectarea numelor și a adreselor reclamanților ca utilizatori ai cartelelor SIM preplătite a constituit o ingerință limitată în drepturile acestora. A observat, însă, că legea în cauză conținea garanții suplimentare, atât timp cât persoanele se puteau adresa unor organisme de supraveghere a datelor independente pentru a examina cererile de date ale autorităților și pentru a solicita reparații în justiție, dacă era necesar.

Privacy International și alții împotriva Regatului Unit

7 iulie 2020 (decizie privind admisibilitatea)

Reclamanții – un ONG cu sediul la Londra, un furnizor de servicii de internet cu sediul la Londra, o asociație de „hacktiviști” cu sediul în Germania, două societăți cu sediul în Statele Unite care furnizează, servicii de Internet și, respectiv, servicii de comunicație, precum și un furnizor de servicii de internet cu sediul în Coreea de Sud – considerau că, pe o durată nedeterminată, sistemele lor făcuseră obiectul unei ingerințe cunoscute sub numele de „hacking” din partea Government Communications Headquarters (GCHQ, Cartierul General pentru Comunicații al Guvernului) și/sau Secret Intelligence Service (Serviciul Secret de Informații). Aceștia se plâneau că autoritatea conferită în temeiul art. 7 din Legea privind serviciile de informații² era lipsită de bază legală, că articolul nu conținea nicio cerință privind autorizația judiciară, că în spațiul public nu existau informații despre modul în care acesta putea fi folosit pentru a autoriza o ingerință în sisteme, precum și că nu exista nicio cerință de filtrare pentru a exclude datele nerelevante. Reclamanții mai adăugau că sesizarea Tribunalului pentru Litigii referitoare la Competențele de Investigare nu constituia un recurs efectiv, comisia respectivă nepronunându-se, în procedurile interne, în cazurile ce intrau în cadrul art. 7.

Curtea a declarat **inadmisibile** plângerile reclamanților formulate în temeiul art. 8, art. 10 (libertatea de exprimare), și art. 13 (dreptul la un recurs efectiv) din Convenție, constatând că, în circumstanțele cauzei, reclamanții nu au oferit instanțelor interne, în special Tribunalului pentru Litigii referitoare la Competențele de Investigare, posibilitatea pe care art. 35 (criterii de admisibilitate) din Convenție este, în principiu, destinat să o acorde unui stat contractant, respectiv posibilitatea să soluționeze și, prin urmare, să împiedice sau să remedieze pretinsa încălcare a Convenției invocată împotriva statului respectiv. Curtea a observat în special argumentele generale avansate de reclamanți și a subliniat, de asemenea, în intervențiile terțelor părți că supravegherea denunțată era deosebit de intruzivă și că erau necesare garanții în acest domeniu. În această privință, a reamintit importanța examinării respectării principiilor art. 8 din Convenție atunci când puterile conferite statului sunt obscure, creând un risc de arbitrar, în special atunci când tehnologia disponibilă devine în continuu tot mai sofisticată. Totuși, această importanță sporește, în contextul epuizării căilor

². Art. 7 din Legea din 1994 privind serviciile de informații (*Intelligence Services Act – ISA*) din 1994 permite ministrului de resort să autorizeze o persoană (și fără să riște vreo sancțiune) să săvârșască o faptă în afara insulelor britanice pentru care, dacă ar fi săvârșită în Regatul Unit, ar fi trasă la răspundere penală.

de atac interne, necesitatea de a oferi instanțelor interne posibilitatea de a se pronunța asupra unor astfel de aspecte, atunci când au potențialul de a face acest lucru.

Big Brother Watch și alții împotriva Regatului Unit

21 februarie 2013 (hotărâre – Marea Cameră)

Aceste cereri au fost depuse după dezvăluirile făcute de Edward Snowden (fost agent contractual al Agenției Naționale de Securitate a SUA) cu privire la programele de supraveghere și de partajare a informațiilor dintre SUA și Regatul Unit. Cauza privea plângeri ale unor jurnaliști și organizații pentru drepturile omului cu privire la trei regimuri diferite de supraveghere: (1) interceptarea în masă a comunicațiilor; (2) partajarea materialelor interceptate obținute de la guverne și servicii de informații străine; și (3) obținerea de date de comunicații de la furnizorii de servicii de comunicații³.

Marea Cameră a hotărât: în unanimitate, că **a fost încălcat art. 8** din Convenție în ceea ce privește regimul de interceptare în masă; în unanimitate, că **a fost încălcat art. 8** în ceea ce privește regimul de obținere a datelor de comunicare de la furnizorii de servicii de comunicații; cu douăsprezece voturi pentru și cinci voturi împotriva că **nu a fost încălcat art. 8** în ceea ce privește regimul Regatului Unit prin care se solicită materiale interceptate de la guverne străine și servicii de informații; în unanimitate, că **a fost încălcat art. 10** (libertatea de exprimare) din Convenție în ceea ce privește atât regimul de interceptare în masă, cât și regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații; și, cu douăsprezece voturi pentru și cinci împotriva că **nu a fost încălcat art. 10** în ceea ce privește regimul prin care se solicită materiale interceptate de la guverne străine și servicii de informații. Curtea a considerat, în special, că, date fiind numeroasele amenințări cu care se confruntă statele în societatea modernă, operarea unui regim de interceptare în masă nu a încălcat în sine Convenția. Cu toate acestea, un astfel de regim trebuia să facă obiectul unor „garanții de la un capăt la altul”, ceea ce înseamnă că, la nivel național, trebuie efectuată o evaluare în fiecare etapă a procesului în ceea ce privește necesitatea și proporționalitatea măsurilor luate; interceptarea în masă trebuie să facă obiectul unei autorizări independente încă de la început, atunci când obiectul și amploarea operațiunii au fost definite; și că operațiunea trebuie să facă obiectul supravegherii și al unui control *a posteriori* independent. Având în vedere regimul de interceptare în masă operat în Regatul Unit, Curtea a identificat următoarele deficiențe: interceptarea în masă fusese autorizată de ministru, nu de un organism independent de executiv; categoriile de termeni de căutare care defineau tipul de comunicații care puteau deveni susceptibile a fi examinate nu au fost incluse în cererea de emiteră a unui mandat; și termenii de căutare legați de o persoană (adică identificatori specifici, precum o adresă de e-mail) nu făcuseră obiectul unei autorizări interne prealabile. Curtea a constatat, de asemenea, că regimul de interceptare în masă nu conținea suficiente protecții pentru materialele jurnalistice confidențiale. De asemenea, s-a constatat că regimul de obținere a datelor de comunicații de la furnizorii de servicii de comunicații nu fusese prevăzut de lege. Curtea a constatat că regimul prin care Regatul Unit putea solicita informații de la guverne străine și/sau agenții de informații dispuseseră de suficiente garanții pentru a proteja împotriva abuzurilor și pentru a garanta că autoritățile din Regatul Unit nu utilizaseră astfel de cereri ca o modalitate de a eluda atribuțiile care le reveneau în temeiul dreptului intern și al Convenției.

Centrum För Rättvisa împotriva Suediei

21 februarie 2013 (hotărâre – Marea Cameră)

Prezenta cauză privea pretinsul risc ca comunicațiile fundației reclamante să fi fost sau să fie interceptate și examinate prin intermediul informațiilor pe baza semnalelor electromagnetice, întrucât aceasta comunica zilnic cu persoane, organizații și companii din Suedia și din străinătate prin e-mail, telefon și fax, adesea pe teme sensibile.

³. La momentul faptelor, regimul de interceptare în masă și de obținere a datelor de comunicații de la furnizorii de servicii de comunicații avea ca bază legală Legea din 2000 privind competențele de investigare. Aceasta a fost înlocuită între timp de Legea din 2016 privind competențele de investigare. Constatările Marii Camere privesc doar dispozițiile legii din 2000, care fusese cadrul juridic în vigoare la momentul faptelor denunțate.

Marea Cameră a hotărât, cu cincisprezece voturi pentru și două împotriva, că, în speță, **a fost încălcat art. 8** din Convenție. A constatat în special că, deși principalele caracteristici ale regimului de interceptare în masă suedez îndeplineau cerințele Convenției privind calitatea legii, regimul suferea totuși de trei carențe: absența unei reguli clare privind distrugerea materialelor interceptate care nu conțineau date cu caracter personal; absența unei cerințe în Legea privind informațiile pe baza semnalelor electromagnetice sau alte acte legislative relevante ca atunci când era luată decizia de a transmite materiale de informații partenerilor străini, erau luate în considerare interesele legate de viața privată a persoanelor; și absența unui control *a posteriori* efectiv. Ca urmare a acestor deficiențe, sistemul nu îndeplinea cerința garanțiilor „de la un capăt la altul”, depășea marja de apreciere lăsată statului pârât în această privință și, în general, nu proteja împotriva riscului de arbitrar și abuzuri.

Ekimdjiev și alții împotriva Bulgariei

11 ianuarie 2022 (hotărâre)

Reclamanții – doi avocați și două organizații neguvernamentale – pretindeau, în special, că, în temeiul sistemului de supraveghere secretă din Bulgaria, comunicațiile oricărei persoane din țară puteau fi interceptate și că, potrivit sistemului de retenție și accesare ulterioară a datelor de comunicații, datele de comunicații ale oricărei persoane din țară puteau fi accesate de autorități. Aceștia susțineau că legile care reglementau aceste două aspecte, astfel cum erau aplicate în practică, nu prevedeau suficiente garanții împotriva supravegherii arbitrare sau abuzive secrete și a accesului la datele de comunicații.

Curtea a hotărât că **a fost încălcat art. 8** din Convenție în ceea ce privește supravegherea secretă, constatând că legislația relevantă care reglementa supravegherea secretă, în special cea aplicată în practică, nu îndeplinea cerințele privind calitatea legii din Convenție și nu era în măsură să mențină supravegherea doar la ceea ce era necesar. A hotărât, de asemenea, că **a fost încălcat art. 8** în ceea ce privește retenția și accesul la datele de comunicații, constatând că, întrucât legile care guvernau retenția și accesul la datele de comunicații nu îndeplineau cerințele de calitate a legii prevăzute de Convenție, acestea nu erau în măsură să limiteze o astfel de retenție și accesul la ceea ce era necesar. În plus, în această hotărâre, Curtea a subliniat faptul că, în temeiul **art. 46** (forța obligatorie și executarea hotărârilor) din Convenție, un stat parte trebuia să facă modificările necesare la dreptul intern pentru a pune capăt încălcării și pentru a restabili, pe cât posibil, situația care ar fi putut fi obținută dacă aceasta nu ar fi avut loc și pentru a se asigura că legile sale sunt compatibile cu Convenția. În prezenta cauză, măsurile trebuiau să le completeze pe cele pe care autoritățile bulgare le luaseră deja pentru a pune în aplicare hotărârea *Asociația pentru Integrare Europeană și Drepturile Omului și Ekimdjiev împotriva Bulgariei* din 28 iunie 2007.

Haščák împotriva Slovaciei

23 iunie 2022 (hotărâre)

Cauza privea o operațiune de supraveghere („operațiunea Gorilla”) efectuată în 2005 și 2006 de serviciul de informații slovac (SIS) și materialul de informații obținut de acesta. Reclamantul – un important om de afaceri asociat unui influent grup financiar și partener de afaceri al reclamantului din cauza [Zoltán Varga împotriva Slovaciei](#) (hotărâre din 20 iulie 2021) – se plângea, în special, de lipsa unei supravegheri și evaluări efective a punerii în aplicare a două mandate de supraveghere emise de Tribunalul Regional din Bratislava la jumătatea anilor 2000, că cadrul aplicabil nu oferea protecție persoanelor afectate în mod aleatoriu de măsurile de supraveghere și că regulile interne aplicabile retenției materialelor de informații nu erau adecvate.

Curtea a considerat că a fost încălcat art. 8 din Convenție în ceea ce privește punerea în aplicare a celor două mandate și retenția materialului analitic. În primul rând, a afirmat că, într-o măsură semnificativă, plângerile reclamantului formulate în temeiul art. 8 erau identice și erau apărute dintr-un antecedent factual și procedural identic cu cel examinat în cauza [Zoltán Varga](#). Prin urmare, a aplicat această jurisprudență în speță. Deși exista o bază legală, Curtea a observat, în special, că operațiunea prezenta numeroase deficiențe,

dintre care unele fuseseră recunoscute la nivel intern ca răspuns la plângerile și acțiunile domnului Varga. Deși instanțele interne nu ajunseseră la astfel de constatări în cazul individual al reclamantului, erau relevante pentru evaluarea cauzei acestuia. Curtea a reamintit că, la fel ca în *Zoltán Varga*, atunci când pusese în aplicare mandatele de supraveghere, SIS se bucurase practic de o putere discreționară echivalentă cu o putere nelimitată, care nu fusese însoțită de o măsură de protecție împotriva unor ingerințe arbitrare, astfel cum prevede statul de drept. În plus, această situație fusese agravată de fapta necontestată că reclamantul nu era el însuși ținta supravegherii în primul din cele două mandate, în lumina argumentului său necontestat potrivit căreia legea nu oferea protecție persoanelor afectate în mod aleatoriu de măsurile de supraveghere și de incertitudinea fundamentală legată de starea practică și procedurală a înregistrării audio recuperate în 2018, probabil de proveniență SIS. În sfârșit, Curtea a amintit că hotărâse anterior în *Zoltán Varga* că stocarea materialului analitic obținut în operațiunea de supraveghere făcuse obiectul unor reguli confidențiale aplicate în lipsa unui control extern. Prin urmare, retenția nu fusese prevăzută de lege. Curtea a decis că acest lucru se aplica și în speță.

A se vedea, de asemenea, printre deciziile recente:

[Ringler împotriva Austriei](#)

12 mai 2020 (Comitetul – decizie privind admisibilitatea)

[Tretter și alții împotriva Austriei](#)

29 septembrie 2020 (Comitetul – decizie privind admisibilitatea)

Cereri pendinte

[Association confraternelle de la presse judiciaire împotriva Franței și alte 11 cereri \(nr. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 și 59621/15\)](#)

Cereri comunicate Guvernului francez la 26 aprilie 2017

Aceste cereri, care au fost formulate de avocați și jurnaliști, precum și de persoane juridice care au legătură cu aceste profesii, privesc legea franceză privind informațiile din 24 iulie 2015.

Curtea a comunicat cererile guvernului francez și a adresat întrebări părților în temeiul art. 8 (dreptul la respectarea vieții private și a corespondenței), art. 10 (libertatea de exprimare) și art. 13 (dreptul la un recurs efectiv) din Convenție.

Cereri similare pendinte: **[Follorou împotriva Franței \(nr. 30635/17\) și Johannes împotriva Franței \(nr. 30636/17\)](#)**, comunicate guvernului francez la 4 iulie 2017.

[Pietrzak împotriva Poloniei și Bychawska-Siniarska și alții împotriva Poloniei \(nr. 72038/17 și 25237/18\)](#)

Cereri comunicate guvernului polonez la 27 noiembrie 2019

Prezenta cauză privește compatibilitatea legislației naționale care autorizează supravegherea secretă de către poliție și serviciile de informații în ceea ce privește comunicațiile și colectarea datelor referitoare la aceste comunicații („metadate”) cu cerințele art. 8 (dreptul la respectarea vieții private și de familie, a domiciliului și a corespondenței) și ale art. 13 (dreptul la un recurs efectiv) din Convenție.

[Cererile](#) au fost comunicate guvernului polonez, împreună cu întrebările Curții, în noiembrie 2019.

Unsprezece terți intervenienți au primit permisiunea de a participa la procedura scrisă; dintre aceștia, patru au fost invitați să participe la ședința Camerei care a avut loc în Palatul Drepturilor Omului la 27 septembrie 2022.

A.L. împotriva Franței (nr. 44715/20) și E.J. împotriva Franței (nr. 47930/21)

Cereri comunicate guvernului francez la 8 decembrie 2021

Aceste aplicații privesc, în special, infiltrarea de către autoritățile franceze a rețelei de comunicații criptate „EncroChat” și capturarea, copierea și analiza datelor stocate și schimbate cu dispozitivele conectate la această rețea.

Curtea a comunicat cererile guvernului francez și a adresat întrebări părților în temeiul art. 6 § 1 (dreptul la un proces echitabil), art. 8 (dreptul la respectarea vieții private și a corespondenței), art. 13 (libertatea de exprimare) art. 34 (dreptul de a introduce o cerere individuală) și art. 35 (condiții de admisibilitate) din Convenție.

Pentru informații suplimentare

A se vedea, în special:

- **„Protectia datelor cu caracter personal”**, fișă tematică întocmită de Biroul de presă al Curții
- **Securitatea națională și jurisprudenta Curtii Europene a Drepturilor Omului**, raport întocmit de Divizia Cercetare a Curții, 2013

Contact presă:

Tel.: +33 (0)3 90 21 42 08