

Accesul la căile de atac în domeniul protecției datelor cu caracter personal în statele membre ale UE

Rezumat

Articolul 8 din Carta drepturilor fundamentale a Uniunii Europene garantează oricărei persoane din Uniunea Europeană (UE) dreptul la protecția propriilor date cu caracter personal. Articolul prevede tratarea acestor date în mod echitabil, în scopuri bine precizate. Asigură oricărei persoane dreptul de acces la propriile date cu caracter personal, precum și dreptul de a obține rectificarea acestora. Articolul 8 prevede faptul că respectarea acestor norme se supune controlului unei autorități independente. Articolul 47 garantează dreptul la o cale de atac eficientă, inclusiv la o audiere echitabilă, publică, într-un interval de timp rezonabil.

Încălări ale protecției datelor se pot produce și chiar se produc aproape pretutindeni: la locul de muncă, în supermarket sau în timp ce navigați pe internet. Aceste situații pot cauza stres emoțional și pot afecta reputația sau relațiile unei persoane.

„Consecințele [încălării secretului în practica medicală] au fost dezastruoase. Toate persoanele în care aveam încredere s-au îndepărtat – părinți, îngrijitori, doctori. În joc era pierderea autodeterminării mele. [...] Întreaga mea lume se prăbușise și rămăsesem singur, fără bani și fără sprijin.” (victimă a unui caz de încălcare a protecției datelor care nu a recurs la nicio cale de atac, Germania)

Cei care s-au confruntat cu astfel de încălări au dreptul să recurgă la căi de atac. Aceștia se pot adresa autorității naționale de protecție a datelor sau alternativelor disponibile pentru a depune plângeri sau a solicita reparații. Multe persoane recurg la căi de atac pentru a evita ca alte persoane să fie afectate în mod similar sau pentru a obține recunoașterea încălării drepturilor acestora. Totuși, este posibil ca aceste persoane să fie descurajate să depună o plângere deoarece se tem că procedurile vor fi prea lungi, prea complexe sau prea costisitoare, îndeosebi în cazul în care acestea presupun reprezentare legală. De asemenea,

este posibil ca aceste persoane să nu reușească să accedă la expertiza sau la sfaturile de care au nevoie.

Acest proiect realizat de FRA prezintă o analiză comparativă la nivelul UE a căilor de atac disponibile ca mijloace de garantare a drepturilor cetățenilor în domeniul protecției datelor. Proiectul se axează pe împletirea a două drepturi fundamentale garantate de Carta drepturilor fundamentale a Uniunii Europene: dreptul la protecția datelor cu caracter personal (articolul 8) și dreptul la o cale de atac eficientă (articolul 47). Dreptul la o cale de atac este o condiție prealabilă obligatorie pentru aplicarea și implementarea eficientă a tuturor celorlalte drepturi fundamentale, inclusiv a dreptului la protecția datelor. Ca atare, este important ca cele două drepturi fundamentale să fie luate în considerare împreună.

„Cred că singurul remediu pe care l-am putut vedea ca fiind încurajator este recunoașterea faptului că li s-a făcut o nedreptate, sau primirea unei decizii prin care se recunoaște că «ceea ce ți s-a întâmplat nu a fost în regulă, drepturile tale au fost încălcate.» (reprezentantă a unei organizații de sprijin pentru victime, România)

Studiul social și juridic realizat de FRA examinează utilizarea și aplicarea căilor de atac în domeniul protecției datelor personale, precum și obstacolele întâlnite în căutarea unei căi de atac eficiente în cazurile de încălcare a protecției datelor. Pe baza datelor de cercetare, FRA identifică punctele deficitare și propune modalități de eliminare a acestora, cu scopul de a contribui la reformarea în curs de desfășurare a regimului de protecție a datelor din UE.

Acest rezumat prezintă concluziile principale ale studiului realizat de FRA, care sunt publicate integral în documentul *Access to data protection remedies in EU Member States* (Accesul la căile de atac în domeniul protecției datelor în statele membre ale UE) (a se vedea „Informații suplimentare”).

Context juridic

Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date (Directiva UE privind protecția datelor) garantează disponibilitatea căilor de atac privind protecția datelor în statele membre ale UE, solicitând fiecărui stat membru să înființeze o autoritate de supraveghere independentă.

În 2012, mânăta de dorința unei aplicări mai eficiente a dreptului fundamental la protecția datelor cu caracter personal, Comisia Europeană a propus o reformă

cuprinzătoare a normelor UE în materie de protecție a datelor. Pachetul de reformă constă într-o propunere de regulament general privind protecția datelor, care să înlocuiască Directiva privind protecția datelor cu caracter personal, precum și o propunere de directivă generală privind protecția datelor, care să înlocuiască Decizia-cadru privind protecția datelor din 2008.

Pachetul de reformă propus vizează consolidarea independenței autorităților naționale de protecție a datelor și a prerogativelor acestor autorități de a remedia încălcări.

Descriere și categorii de persoane intervievate

Toate citatele care apar în rezumat sunt preluate din raportul integral *Access to data protection remedies in EU Member States* (Accesul la căile de atac în domeniul protecției datelor în statele membre ale UE). Pentru a spori claritatea rezumatului, FRA a modificat categoriile corespunzătoare persoanelor citate. În rezumat se face trimitere la sursa citată ca la o „victimă a unui caz de încălcare a protecției datelor care nu a recurs la nicio cale de

atac”, aceasta apărând în raportul integral cu denumirea juridică de „persoană care nu a făcut plângere”. În mod similar, victimele care au recurs la remedii juridice sunt menționate în raportul integral ca „reclamanți”. FRA a intervievat, de asemenea, persoane care lucrează în cadrul organizațiilor de sprijin pentru victimele încălcării protecției datelor, inclusiv grupuri precum organizații ale angajaților, sindicate sau organizații care tratează plângeri. În rezumat sunt specificate rolurile acestora; în raportul integral, aceste persoane sunt denumite „intermediari”. „Avocații” și „judecătorii” sunt menționați ca atare atât în rezumat, cât și în raportul integral.

Tabel: Numărul persoanelor intervievate și al participanților la discuțiile grupurilor tematice

	Numărul persoanelor intervievate			Numărul participanților la grupurile tematice sau la interviuri		
	Reclamanți	Persoane care nu au făcut plângere	Judecători/procurori	Personal APD	Intermediari	Avocați practicanți
<i>Număr minim planificat</i>	30-40			6	6	6
Austria	7	6	5	2	7	8
Bulgaria	16	14	8	6	2	3
Finlanda	24	6	6	8	6	6
Franța	25	9	5	6	7	8
Germania	20	6	5	6	5	4
Grecia	16	15	4	7	7	5
Italia	2	9	6	7	7	7
Letonia	5	2	2	5	5	4
Polonia	15	15	6	8	8	6
Portugalia	7	7	6	2	3	4
Regatul Unit	28	2	6	10	9	4
Republica Cehă	4	6	5	10	6	6
România	4	2	3	0	6	3
Spania	11	3	4	5	6	6
Țările de Jos	24	9	7	6	6	5
Ungaria	13	19	6	9	6	5
Total	351		84	97	96	84

Colectarea datelor și acoperire

Pentru acest studiu, FRA a examinat cadrul legal privind protecția datelor din cele 28 de state membre ale UE, analizând legile și regulamentele de procedură pentru a prezenta o analiză comparativă a situației juridice a protecției datelor în UE.

În perioada aprilie-septembrie 2012, Franța, rețeaua de cercetare multidisciplinară a FRA, a desfășurat o cercetare de teren calitativă în 16 state membre ale UE: Austria, Bulgaria, Republica Cehă, Finlanda, Franța, Germania, Grecia, Ungaria, Italia, Letonia, Țările de Jos, Polonia, Portugalia, România, Spania și Regatul Unit. Peste 700 de persoane din șase

grupuri-țintă au fost intervievate sau au luat parte la grupuri tematice. Cele șase grupuri-țintă au fost formate din: reclamanți sau victime în cazuri de încălcare a protecției datelor care au recurs la o cale de atac; persoane care nu au făcut plângere, de exemplu victime presupuse ale unor cazuri de încălcare a protecției datelor care au hotărât să nu recurgă la căi de atac; judecători; personal din cadrul autorităților de protecție a datelor; intermediari, inclusiv membri ai personalului organizațiilor societății civile care asigură sprijin pentru persoanele care s-au confruntat cu încălcări ale protecției datelor; și avocați practicanți.

Constatări principale și sfaturi bazate pe dovezi

Pe baza constatărilor sale, FRA întrevide posibilități concrete pentru ca instituțiile UE, statele membre și mecanismele implicate în aplicarea căilor de atac privind protecția datelor să îmbunătățească disponibilitatea și calitatea acestora pentru victimele cazurilor de încălcare a protecției datelor din UE. În acest context, FRA recomandă mai multe etape pentru sprijinirea instituțiilor UE și a factorilor de decizie naționali în ceea ce privește elaborarea și punerea în aplicare de măsuri concepute pentru garantarea protecției datelor cu caracter personal și pentru solicitarea de reparații în cazuri de încălcare.

Cunoașterea propriilor drepturi: sensibilizarea opiniei publice

O sensibilizare mai mare a opiniei publice cu privire la dreptul la protecția datelor, tipurile de încălcări ale acestui drept, mecanismele de reparație și modul în care se poate beneficia de acestea contribuie, de asemenea, la eficiența căilor de atac. Publicul trebuie să poată recunoaște o încălcare a protecției datelor pentru a recurge la o cale de atac.

Acest studiu al FRA a analizat diferitele tipuri de încălcări, persoanele care le săvârșesc și impactul acestor încălcări asupra victimelor. De asemenea, studiul a examinat ce anume motivează victimele să recurgă la căi de atac.

Tipuri de încălcări în domeniul protecției datelor cu caracter personal

Activitățile desfășurate pe internet, marketingul direct și supravegherea video care utilizează în secret televiziunea cu circuit închis (CCTV) apar, în cadrul cercetării de teren, ca fiind cele mai frecvente surse ale încălcărilor protecției datelor. Cel mai adesea se fac vinovate de aceste încălcări organismele guvernamentale, agențiile de aplicare a legii, precum și instituțiile financiare și cele medicale.

Cele mai frecvente cazuri de încălcare a protecției datelor, menționate în timpul cercetării de teren, vizează activitățile desfășurate pe internet. Acestea includ platformele sociale, cumpărăturile online, scurgerea de date cu caracter personal din magazinele online, spargerea conturilor de e-mail și a bazelor de date, furtul identității, încălcarea securității și utilizarea necorespunzătoare a datelor cu caracter personal de către societățile de internet globale. Activitățile desfășurate pe internet se remarcă, din punctul de vedere al protecției datelor, ca un teritoriu cu grad ridicat de risc.

O altă încălcare frecventă a protecției datelor este reprezentată de marketingul direct și de cercetarea de piață fără consimțământul destinatarului, atunci când datele cu caracter personal sunt utilizate în mod abuziv fie pe telefoanele mobile, fie prin e-mail ori prin poștă. Operatorii de telefonie mobilă și instituțiile de colectare a datoriei sunt, adesea, responsabile de aceste încălcări,

potrivit datelor furnizate în cadrul cercetării de teren. Respondenții au indicat, de asemenea, practici ilicite, precum vânzarea de date cu caracter personal către părți terțe.

Adesea, persoanele intervievate au făcut referire la camerele ascunse de supraveghere video la locul de muncă, în domeniul public sau în supermarketuri. Mai mulți respondenți din diferite țări au declarat că s-au confruntat cu situații de supraveghere secretă efectuată de autoritățile publice și bazată pe tehnologii speciale sau pe CCTV instalate în secret. Mai multe autorități de protecție a datelor, de exemplu în Regatul Unit, au elaborat ghiduri privind utilizarea CCTV.

În ceea ce privește relația specifică angajator-angajat, respondenții menționează, de asemenea, alte cazuri de pretinsă încălcare a protecției datelor. Acestea includ: colectarea datelor cu caracter personal ale angajaților, accesul la datele cu caracter personal stocate pe calculatoarele angajatorilor, utilizarea sistemelor de legitimare și de poziționare globală, utilizarea discriminatorie a datelor cu caracter personal sensibile, colectate prin sondaje sau audituri, precum și divulgarea datelor angajaților de către angajatori.

Cercetarea de teren a indicat, de asemenea, că încălcările financiare sunt foarte frecvente, inclusiv spargerea conturilor bancare sau piratarea cardurilor de credit. În pofida acestui fapt, studiul identifică doar câțiva reclamanti care declară că au suferit pierderi financiare în urma încălcărilor. În multe dintre aceste cazuri, respondenții descriu sumele implicate ca fiind minore, acestea fiind legate de apeluri telefonice, tarife poștale și costuri aferente accesului și modificării datelor înregistrate.

Impactul asupra victimelor

Respondenții descriu daunele suferite ca urmare a încălcării protecției datelor ca fiind de natură psihologică și socială, precum tulburări emoționale sau prejudicierea reputației. De asemenea, mai puțin frecvent, participanții raportează pierderi financiare.

Victimele cazurilor de încălcare a protecției datelor solicită reparații din diverse motive, cum ar fi rectificarea sau ștergerea datelor cu caracter personal ori sancțiuni împotriva infractorilor. Respondenții declară faptul că încearcă să protejeze alte persoane prin prevenirea unor viitoare încălcări și să obțină recunoașterea faptului că a avut loc o încălcare.

Atunci când sunt întrebați cu privire la daunele provocate de încălcarea protecției datelor, reclamantii și persoanele care nu au făcut plângere

de descriu, de cele mai multe ori, ca fiind de natură psihologică sau socială. Aceștia se concentrează fie pe emoții, fie pe măsura în care relațiile sau reputația lor au fost afectate, și menționează diferite grade de tulburări emoționale, confruntări și lipsa siguranței, cum ar fi faptul că se simt persecutați sau supravegheați, menționând chiar și sentimentul de neputință. De asemenea, aceștia descriu daunele la adresa reputației profesionale sau personale, pierderea încrederii și alte forme de daune morale, astfel cum s-a subliniat în studiul efectuat de FRA în urma cercetării de teren, de exemplu în Austria, Bulgaria, Germania, Grecia, Ungaria, Italia, Letonia, Țările de Jos, Polonia și Spania. Un reclamant din Spania caracterizează un aspect al acestui sentiment ca fiind „o neputință în fața unui abuz de putere”.

„Am părăsit locul de muncă în condiții foarte dificile. [...] Mă durea sufletul [...] și nu mă puteam apăra deoarece nu știam dacă aceste acuzații existau.” (victimă a unui caz de încălcare a protecției datelor care a recurs la o cale de atac, Grecia)

Persoanele intervievate din Republica Cehă, Italia, Țările de Jos, Portugalia și România menționează daune suferite ca urmare a încălcărilor în ceea ce privește relațiile de muncă, de exemplu proceduri disciplinare, suspendări și/sau rezilierea contractului de muncă sau riscul concedierii. În unele dintre aceste cazuri, daunele vizează pierderi financiare, inclusiv ratarea unor oportunități profesionale, imposibilitatea obținerii unui împrumut bancar, lipsa dreptului la asistență medicală sau la prestații sociale, costuri ridicate ale reprezentării legale sau pierderi financiare imediate și perspective de pierderi financiare prin asumarea ilicită a responsabilităților.

Unii respondenți solicită reparații pentru a-și soluționa, în principal, situația personală. Un procent mult mai mare urmărește prevenirea încălcărilor care pot afecta alte persoane în viitor, obținerea recunoașterii încălcării sau încetarea încălcărilor ori sancționarea infractorului. Compensarea financiară nu este un motiv predominant pentru solicitarea de reparații. Cel mai frecvent, respondenții menționează „prevenirea unor noi încălcări ale drepturilor”, „sensibilizarea publicului”, „încetarea practicilor incorecte”, „apărarea drepturilor fundamentale”, „darea unei lecții [autorităților vizate]”, „obținerea recunoașterii încălcării din partea unei autorități competente” sau „sancționarea infractorului”.

Deși respondenții subliniază lipsa de informare cu privire la problema încălcării protecției datelor în rândul profesioniștilor, dar și al victimelor, mai multe state membre ale UE dispun, de asemenea, de programe de sensibilizare a publicului.

Opinia FRA

Victimele nu sunt conștiente de încălcări în domeniul protecției datelor personale și de căile de atac disponibile. Aceste constatări obținute în urma cercetării de teren confirmă concluziile studiilor existente ale FRA.

După cum s-a recunoscut în raportul FRA din 2010 privind Protecția datelor în Uniunea Europeană, sensibilizarea publicului cu privire la legislația privind protecția datelor este o sarcină importantă pentru instituțiile relevante, precum autoritățile naționale de protecție a datelor. Raportul FRA din 2012 privind Accesul la justiție în cazurile de discriminare și opinia FRA din 2013 cu privire la directivele UE privind egalitatea au subliniat o lipsă de informare similară în ceea ce privește legislația UE privind nediscriminarea. Măsurile de sensibilizare sunt necesare pentru toată lumea, de la publicul larg la judecători. Cunoștințele privind organizațiile de sprijin cărora li se pot adresa reclamații atunci când înaintează plângeri legate de protecția datelor trebuie extinse în mod semnificativ în întreaga Uniune Europeană.

UE ar putea promova și, eventual, sprijini din punct de vedere financiar campaniile de sensibilizare la nivelul statelor membre ale UE. Pentru a sensibiliza actorii naționali relevanți cu privire la normele de protecție a datelor, în colaborare cu Consiliul Europei și cu Curtea Europeană a Drepturilor Omului, FRA a elaborat un Manual privind legislația europeană în materie de protecție a datelor.

Statele membre ale UE ar putea avea în vedere adoptarea măsurilor necesare pentru o mai mare sensibilizare a publicului cu privire la existența și funcționarea mecanismelor disponibile pentru depunerea plângerilor, îndeosebi cu privire la autoritățile de protecție a datelor. În plus, autoritățile de protecție a datelor ar trebui să acorde o atenție deosebită cultivării profilurilor lor publice în calitate de gardieni independenți ai dreptului fundamental la protecția datelor, precum și să își consolideze activitățile de sensibilizare cu privire la protecția datelor.

Recurgerea la căile de atac: consolidarea autorităților de protecție a datelor

Pentru cei care recurg la căi de atac în legătură cu încălcarea drepturilor la protecția datelor, autoritățile de protecție a datelor s-au dovedit cele mai populare și, în multe cazuri, singura opțiune relevantă pentru solicitarea de reparații. Pentru a răspunde acestei cereri, autoritățile respective trebuie să fie împuternicite pentru a oferi servicii solide și cuprinzătoare.

Directiva privind protecția datelor din 1995 stabilește puterile autorităților de protecție a datelor, acestora fiindu-le acordate competențe de investigare și intervenție în scopul prevenirii încălcărilor. Aceste autorități joacă un rol important în remedierea încălcărilor protecției datelor, acționând adesea ca prim punct de contact pentru victimele unor astfel de încălcări. Acest rol este frecvent recunoscut de instanțele judecătorești naționale; în Finlanda, de exemplu, procurorii și instanțele au obligația de a oferi autorității de protecție a datelor posibilitatea de a fi audiată în cazuri care vizează un comportament contrar Legii privind datele cu caracter personal din Finlanda.

Consolidarea rolului autorităților de protecție a datelor

Unele dintre principalele critici aduse de intermediari autorităților naționale de protecție a datelor vizează comunicarea deficitară, un grad insuficient de transparență și contribuția scăzută la sensibilizarea publicului. De asemenea, unii pun sub semnul întrebării independența autorităților, în principal din cauza unor posibile numiri pe criterii politice.

Chiar personalul autorităților de protecție a datelor a ridicat problema forței executorii a deciziilor autorităților, care se leagă de competențele lor limitate în ceea ce privește asigurarea punerii în aplicare a deciziilor, inclusiv de prelucrarea ilegală a datelor cu caracter personal de către administrațiile publice. Potrivit reprezentanților autorităților naționale de protecție a datelor, lipsa de resurse umane și financiare împiedică funcționarea practică a căilor de atac și subminează calitatea activității lor.

Autoritățile de protecție a datelor pot emite ordine de corectare a încălcărilor protecției datelor sau pot aplica amenzi, deși competențele acestora de corectare a unor astfel de încălcări și măsura în care acestea le folosesc variază la nivelul statelor membre ale UE. Aceste competențe includ avertismente oficiale, ordine specifice, ordonanțe, revocarea licențelor, amenzi, alte sancțiuni pecuniare sau deferirea cazului în fața instanței sau a parchetului relevant din statul membru în cauză.

„Uneori, oamenii se plâng de procedura prin avocatul poporului și în aceste cazuri oamenii chiar nu știu care este scopul și obiectivul unei astfel de proceduri și care sunt limitele noastre. Atunci le explicăm, desigur, spunându-le că «nu putem pur și simplu să mergem acolo, de exemplu, și să tăiem cablul camerei video». Da, uneori pur și simplu se înțelege greșit procedura și respectiva persoană chiar trebuie să se adreseze instanței.” (membru al personalului autorității de protecție a datelor, Austria)

Autoritățile judiciare din majoritatea statelor membre ale UE pot impune sancțiuni penale sub forma unei amenzi sau a privării de libertate. Durata sentinței și valoarea amenzii variază de la un stat membru al UE la altul. Pentru unii participanți la cercetarea de teren socială, mai concret pentru judecătorii din Grecia, gravitatea sancțiunilor contribuie la eficiența procedurilor judiciare.

Potrivit datelor din 19 state membre ale UE, cel mai adesea autoritățile de protecție a datelor aplică o amendă sau o sancțiune pecuniară în cazul unei încălcări a protecției datelor, deși dispun, în mod obișnuit, de o serie de măsuri. Adesea, legislația națională stabilește valoarea amenzii impuse și multe state membre ale UE fac distincția între persoane fizice sau indivizi și persoane juridice sau organisme corporative. Deseori, amenzile pot fi majorate pentru a pedepsi persoanele care recidivează sau pentru cazurile în care au fost comise numeroase încălcări.

„Criticile vizează, în principal, nu atât faptul că nu dispunem de independență, ci mai ales faptul că protecția datelor nu funcționează. Atunci când nu obținem reparații, reclamantul exclamă: «Să nu mai aud de protecția datelor!». Aceasta este imaginea unui tigru fără dinți, a unui tigru care nu poate să muște. [...] Din acest motiv, competența de a emite ordine a fost importantă pentru noi; ceea ce contează este să ai rezultate și să pui în aplicare diverse opțiuni, nu numai să aplici amenzi.” (membru al personalului autorității de protecție a datelor, Germania)

Adoptarea propunerii de regulament al Comisiei Europene ar consacra în legislația UE competența acestor autorități de a impune sancțiuni administrative, și anume amenzi și alte sancțiuni pecuniare. Deși majoritatea autorităților de protecție a datelor dispun deja de această competență, constatările FRA indică faptul că regulamentul propus ar extinde în mod semnificativ domeniul de aplicare pentru a include sancțiuni cu o valoare mai mare, până la maximum 1 000 000 EUR sau 2 % din cifra de afaceri globală anuală a unei întreprinderi.

Solicitarea de reparații prin intermediul autorităților de protecție a datelor

Majoritatea reclamantilor din cele 16 state membre ale UE vizate de studiu au ales să solicite reparații prin intermediul autorității naționale de protecție a datelor. De asemenea, aceasta a fost opțiunea preferată a celor care au avut în vedere solicitarea de reparații, dar care, din diverse motive, au ales să nu dea curs acțiunii. Reclamantii declară că au optat pentru autoritatea de protecție a datelor în detrimentul altor alternative din mai multe motive, printre care: costuri mai mici, durată mai redusă a procedurilor, grad mai scăzut de complexitate a procedurilor, posibilitatea ca persoanele fizice, fără reprezentare legală, să inițieze și să facă uz de procedură, consultanța primită, competența autorităților, precum și disponibilitatea limitată a altor proceduri.

Reclamantii incluși în studiu au fost mai reticenti în ceea ce privește inițierea unor proceduri judiciare din cauza costurilor mai ridicate, a procedurilor mai îndelungate și a nevoii percepute de a fi reprezentat sau asistat de un avocat. Măsurile penale joacă un rol în anumite cazuri, dar sunt rareori folosite în statele membre ale UE vizate de studiu, cu unele excepții notabile.

„În acel moment nu m-am gândit la reparații sau compensații. Eram nemulțumit de faptul că, dacă a primit datele tale, o întreprindere crede că poate face orice cu ele. Voiam să pun capăt acestei practici. Voiam ca datele mele să fie șterse.” (victimă a încălcării protecției datelor care a recurs la o cale de atac, Letonia)

Alegerea mecanismului de reparație depinde de informațiile disponibile, care, de obicei, sunt insuficiente, precum și de consultanța primită. Pe baza informațiilor de care dispun cu privire la aceste aspecte, persoanele care au fost victime în cazuri de încălcare a protecției datelor pot fi clasificate în două grupe. Majoritatea persoanelor intervievate declară că nu dispun de informații. A doua grupă, o minoritate de persoane intervievate „bine informate”, declară că dispun de informații suficiente datorită mediului de lucru, de obicei juridic, sau grație experienței anterioare.

Opinia FRA

Autoritățile de protecție a datelor, principalii actori care protejează drepturile de protecție a datelor, joacă un rol esențial în tratarea majorității coplesitoare a plângerilor legate de protecția datelor. Este nevoie de măsuri suplimentare pentru a garanta că accesul la autoritățile de protecție a datelor este aplicat efectiv.

Independența autorităților de protecție a datelor trebuie consolidată printr-o reformă a legislației UE. Autoritățile de protecție a datelor ar trebui să dispună de competențe și prerogative consolidate, bazate pe resurse umane și financiare adecvate, inclusiv specialiști în diverse domenii și practicieni calificați, cum ar fi specialiști formați în domeniul tehnologiei informației și avocați specializați.

Parlamentul European și Consiliul Uniunii Europene propun un regulament pentru protecția cetățenilor cu privire la prelucrarea datelor cu caracter personal și libera circulație a unor astfel de date. Regulamentul general privind protecția datelor vizează armonizarea legislației privind protecția datelor și consolidarea capacității autorităților de protecție a datelor de a corecta încălcările.

Consolidarea protecției datelor ar putea include garanții pentru aplicarea efectivă a deciziilor lor și durate rezonabile ale procedurilor [a se vedea, de asemenea, în contextul specific al nediscriminării, raportul FRA 2012 Access to justice in cases of discrimination in the EU: steps to further equality (Accesul la justiție în cazurile de discriminare din UE: pași către mai multă egalitate)]. Acestea ar permite autorităților de protecție a datelor să se mențină ca punct preferat de acces pentru cazurile de încălcare a protecției datelor, simplificând, în același timp, căile existente de atac și reducând costurile generale, întârzierile și formalitățile [a se vedea FRA Opinion on the proposed data protection reform package (Avizul FRA din 2012 privind pachetul de reformă propus pentru protecția datelor)].

Pentru consolidarea autorității și a credibilității lor, autoritățile de protecție a datelor ar trebui să joace un rol important în aplicarea sistemului de protecție a datelor, dispunând de competența emiterii de sancțiuni sau a inițierii procedurilor care pot conduce la sancțiuni [a se vedea, de asemenea, raportul FRA 2010 Data protection in the European Union: the role of national data protection authorities (Protecția datelor cu caracter personal în Uniunea Europeană: rolul autorităților naționale de protecție a datelor)].

Acest aviz este în acord cu rezultatele obținute în contextul altor organisme nejudiciare, precum organismele de promovare a egalității, astfel cum se subliniază în Avizul FRA din 2013 cu privire la directivele UE privind egalitatea (pagina 3):

„Gradul în care procedurile de depunere a plângerilor își îndeplinesc rolul de reparare a daunelor cauzate și de descurajare a infractorilor depinde de măsura în care organele de soluționare a litigiilor pot emite sancțiuni eficiente, proporționale și disuasive” și „dacă organizațiile societății civile, inclusiv organismele de promovare a egalității, ar putea introduce plângeri în instanță sau ar putea derula anchete, [...] aplicarea ar putea fi facilitată”.

Autoritățile de protecție a datelor sunt încurajate să fie mai transparente, precum și să comunice în mod eficient cu publicul larg, oferind informațiile necesare și facilitând, în practică, accesul la căile de atac. În plus, astfel cum se subliniază în Raportul FRA 2010 privind rolul autorităților naționale de protecție a datelor din UE, autoritățile de protecție a datelor „ar trebui să promoveze o cooperare și o sinergie mai strânsă cu alți gardieni ai drepturilor fundamentale [...] în cadrul arhitecturii emergente a drepturilor fundamentale în UE” (pagina 8). Aceste etape ar îmbunătăți imaginea autorităților de protecție a datelor, eficiența și independența percepute ale acestora, precum și încrederea publicului larg.

Obținerea de sprijin: consolidarea rolului organizațiilor societății civile

În cadrul cercetării de teren, organizațiile societății civile s-au dovedit a fi o sursă importantă de informații, consultantă, asistență juridică și reprezentare, asigurând contribuții de valoare pentru cadrul statutar al protecției datelor. De asemenea, aceste organizații asigură sensibilizarea publicului și fac publice chestiunile legate de protecția datelor și

eventuale căi de atac. Totuși, acestea sunt prea puțin numeroase – factor care, în practică, limitează accesul cetățenilor la căi de atac.

Cercetarea de teren indică faptul că există o penurie de organizații ale societății civile care pot oferi servicii cuprinzătoare și bine cunoscute, dezvoltând un profil public în domeniul protecției datelor. Acest fapt limitează accesul în practică al cetățenilor la căi de atac.

„Prin urmare, noi și partenerii noștri oferim consultanță în diverse domenii: juridic, fiscal, cele mai bune achiziții și chiar în ceea ce privește încrederea; atunci când oamenii ne spun că au probleme, încercăm să le transmitem informații privind drepturile lor și instrumentele juridice la care pot recurge pentru soluționarea acestor probleme. Uneori, însă, înaintăm acțiune în justiție, mai ales că dispunem de un instrument de acțiune colectivă, în cazul în care chestiunea poate fi de interes pentru mai multe persoane.” (representant al unei organizații de sprijin al victimelor, Italia)

Cercetarea de teren desfășurată de FRA în 16 state membre ale UE s-a confruntat cu dificultăți în găsirea unor potențiali respondenți care să reprezinte organizații ale societății civile sau intermediari. În cele mai multe dintre țări, a fost dificil să se găsească reprezentanți ai organizațiilor care se ocupau în special de aspecte ale protecției datelor, care asigurau sprijin pentru victimele încălcărilor sau care aveau o experiență extinsă în acest domeniu.

Intermediarii intervievați în cadrul cercetării de teren spun că, în principal, oferă consultanță și informații

persoanelor fizice care au fost victime ale încălcărilor protecției datelor, cu privire la drepturile acestora și la căile de atac disponibile. Aceștia oferă asistență persoanelor fizice în ceea ce privește plângerile acestora. Alte activități menționate de respondenții din cadrul studiului includ educația, cercetarea și formarea. Unii subliniază activitatea de sensibilizare desfășurată prin intermediul campaniilor media, prin articole și publicații, precum și prin monitorizare și activitatea de lobby.

„Prioritatea noastră este să informăm; prin intermediul revistei și al site-ului internet, precum și prin presă și diferite publicații, oferind explicații cu privire la o multitudine de chestiuni, inclusiv la aceasta [protecția datelor] [...] Un al doilea element este că oferim consultanță persoanelor care solicită acest lucru și care sunt interesate; acestea primesc explicații cu privire la drepturile lor și la proceduri. Ulterior, dacă este necesar, trimitem cazurile la autoritățile competente. [...] Următoarea etapă este reprezentarea legală și procedurală, în care ni se acordă dreptul foarte important de a reprezenta consumatorii.” (representant al unei organizații de sprijin al victimelor, Bulgaria)

Opinia FRA

Raportul subliniază importanța organizațiilor intermediare ca surse de informații, consultanță, asistență juridică și reprezentare. Totuși, numai un număr foarte limitat de organizații ale societății civile pot oferi servicii cuprinzătoare victimelor încălcării protecției datelor. UE și statele sale membre ar trebui să mărească finanțarea acordată organizațiilor societății civile și organismelor independente în măsură să ajute victimele care solicită reparații.

Adesea, victimele sunt reticente în ceea ce privește introducerea unei acțiuni în justiție. Un pas important în ceea ce privește punerea în aplicare ar fi să se acorde organizațiilor societății civile permisiunea de a introduce acțiuni în justiție sau de a desfășura anchete. După cum s-a subliniat deja în alte rapoarte și avize ale FRA și după cum s-a confirmat prin constatările din prezentul raport, normele stricte legate de calitatea procesuală împiedică organizațiile societății civile să joace un rol mai direct în litigii, în cazurile de încălcare a drepturilor fundamentale [a se vedea raportul FRA 2011, Access to justice in Europe: an overview of challenges and opportunities (Accesul la justiție în Europa: o prezentare generală a provocărilor și oportunităților) și raportul FRA 2012, Access to justice in cases of discrimination in the EU: steps to further equality (Accesul la justiție în cazurile de discriminare din UE: pași către mai multă egalitate)].

Avizul FRA din 2012 privind pachetul de reformă propus pentru protecția datelor prevede, în special, că UE ar trebui să ia în considerare o nouă relaxare a normelor privind calitatea procesuală pentru a permite organizațiilor care acționează în interes public să înainteze plângeri privind protecția datelor în cazurile în care este puțin probabil ca victimele să introducă o acțiune în justiție împotriva unui organism de control al datelor, având în vedere costurile, stigmatul și alte neplăceri cărora acestea ar trebui să le facă față. Potrivit rapoartelor FRA privind accesul la justiție, acest fapt ar asigura, de asemenea, tratarea cazurilor de importanță strategică, consolidând astfel cultura respectării legislației privind protecția datelor. O astfel de extindere a normelor privind calitatea procesuală ar trebui însoțită de garanții suplimentare care să mențină echilibrul corect între accesul efectiv la căi de atac și abuzul de procedură. În Regulamentul general privind protecția datelor, Comisia a propus o formă de acțiune colectivă de reprezentare.

Depășirea barierelor: reducerea costurilor și ușurarea sarcinii probei

Studiul FRA a vizat identificarea factorilor care împiedică victimele încălcării protecției datelor să recurgă la căi de atac. Pe lângă lipsa unei consultanțe specializate și a unui sprijin din partea experților, studiul indică existența unui număr de obstacole, inclusiv costurile, durata excesivă a procedurilor și dificultățile legate de povara aducerii de probe, îndeosebi pentru încălcările săvârșite prin internet.

Respondenții consideră că o barieră importantă în calea accesului la căi de atac în domeniul protecției datelor o reprezintă costurile implicate, fie procedurale, fie pentru reprezentarea legală. Procedurile îndelungate cu rezultate nesigure tind să majoreze costurile, ceea ce ar putea însemna, de asemenea, că aceste costuri depășesc beneficiile potențiale.

Reclamanții, intermediarii și avocații practicanți intervievați tind, într-o măsură mai mare decât judecătorii intervievați, să identifice povara aducerii de probe ca fiind o problemă. Aceștia vorbesc despre aspectele legate de furnizarea unor dovezi suficiente și complete, în special cu privire la activitățile bazate pe internet.

În mod previzibil, persoanele fizice care au făcut obiectul unor încălcări preferă căi de atac care nu implică niciun cost. Constatările cercetării de teren desfășurate în majoritatea celor 16 state membre ale UE investigate arată faptul că aceste costuri și riscurile asociate se numără printre principalele preocupări ale persoanelor atunci când decid să inițieze sau să continue acțiunea în justiție.

Costul reprezentării legale, de exemplu, este un element care descurajează adesea victimele încălcării protecției datelor să înainteze plângeri. Având în vedere importanța asistenței juridice în cazurile de protecție a datelor, disponibilitatea și accesul la asistența juridică gratuită joacă un rol esențial în decizia urmării unei anumite direcții în materie de căi de atac. Asistența judiciară și alte mijloace care permit ca mecanismele de reparație să fie gratuite contribuie la un grad mai ridicat de accesibilitate a acestor mecanisme pentru un număr mai mare de persoane. Constatările cercetării de teren indică un acces limitat la mecanismele de reparație din cauza limitării asistenței juridice.

„Reclamanții vor să facă tot ce le stă în putință (să inițieze un proces penal sau civil, să solicite o indemnizație, să sesizeze Curtea Supremă), cu condiția să nu plătească nimic; însă, atunci când există costuri, aceștia nu mai doresc să inițieze nicio acțiune, cu excepția sesizării Agenției de protecție a datelor din Spania, o procedură care, deși are limitările sale, este gratuită.” (avocat, Spania)

În cazul în care reprezentarea legală nu este obligatorie, reclamanții pot reduce costurile în mod considerabil, reprezentându-se singuri. Totuși, autoreprezentarea nu este de preferat din cauza complexității acestui domeniu de drept. Însă această opțiune oferă reclamanților care altfel nu ar fi reacționat în acest mod posibilitatea de a introduce acțiuni în justiție.

Costurile ridicate ale procedurilor judiciare reprezintă o preocupare conexasă. Adesea, acestea împiedică reclamanții să sesizeze instanțele, chiar dacă, prin câștigarea procesului, ar putea primi compensații. Respondenții din multe state membre ale UE care au făcut obiectul studiului consideră că nivelul ridicat al costurilor de procedură în acțiunile civile, inclusiv taxele judiciare, reprezintă o problemă; acesta este cazul, de exemplu, în Austria, Franța, Germania, Grecia, Ungaria, Italia, Țările de Jos, Polonia, Portugalia, Spania și Regatul Unit.

„Într-o acțiune civilă ai un avocat, însă nu sunt mulți avocați care să fie familiarizați cu această lege. Dar, dacă ai nevoie de un avocat, procedurile civile sunt prea costisitoare. [...] Procedurile civile costă cel puțin câteva mii de euro și acesta este un preț ridicat.” (judecător, Țările de Jos)

O altă barieră în calea introducerii unei acțiuni în justiție este povara aducerii de probe. Cei mai mulți dintre reclamanții intervievați în cele 16 state membre ale UE vizate de cercetarea de teren menționează dificultăți în ceea ce privește furnizarea unor dovezi complete și suficiente. Reclamanții intervievați în Republica Cehă, Grecia, Letonia, Portugalia, România și Spania indică aducerea de probe ca fiind un obstacol în calea accesării căilor de atac în domeniul protecției datelor. Problemele se axează pe dificultatea dovedirii încălcării protecției datelor, în principal în ceea ce privește activitățile bazate pe internet, și pe mai multe obstacole practice legate de obținerea de dovezi în domeniul specific al protecției datelor. Avocații și intermediarii intervievați împărtășesc această opinie, în timp ce judecătorii, de exemplu din Portugalia și din România, consideră povara aducerii de probe ca fiind acceptabilă.

Opinia FRA

Victimele cazurilor de încălcare a protecției datelor sunt descurajate să introducă acțiuni în justiție din mai multe motive, care includ costurile și dificultățile asociate dovedirii încălcării protecției datelor. Statele membre ale UE ar trebui să ia în considerare promovarea sprijinului prin intermediul centrelor de consultanță juridică sau prin activități pro bono. Aceste mecanisme de sprijin ar trebui să vină în completarea unui sistem de asistență juridică dotat cu resurse adecvate, și nu să substituie un astfel de sistem.

Furnizarea de consultanță: consolidarea specializării juridice în materie de protecție a datelor

Studiul remarcă faptul că există o lipsă de specializare în cadrul profesiei juridice în domeniul protecției datelor cu caracter personal. Pe lângă procedurile îndelungate, complexe și costisitoare, numărul redus de consultanți cu cunoștințe solide determină multe victime să nu recurgă la nicio cale de atac. Consolidarea competențelor profesionale ale avocaților și judecătorilor care activează în domeniul protecției datelor ar facilita disponibilitatea specializării necesare și ar accelera procesul decizional, reducând, în același timp, durata îndelungată a procedurilor.

Chiar și specialiștii în domeniul juridic indică faptul că există prea puțini specialiști în domeniul protecției datelor și că doar un număr redus de cazuri ajung în instanță, aceste comentarii subliniind dificultatea cu care organizatorii proiectului au găsit judecători și avocați care să fie intervievați în cadrul cercetării de teren.

Opinia FRA

Practicienii în domeniul dreptului nu preiau prea des cazuri de protecție a datelor și, prin urmare, nu sunt familiarizați cu procedurile judiciare aplicabile și garanțiile aferente. Există o penurie de judecători specializați în acest domeniu.

UE ar putea sprijini, din punct de vedere financiar, activitățile de formare pentru avocați și judecători cu privire la legislația referitoare la protecția datelor și la punerea acesteia în aplicare la nivelul statelor membre. Statele membre ale UE ar trebui să urmărească consolidarea competențelor profesionale ale judecătorilor și avocaților în domeniul protecției datelor, oferind programe de formare și acordând o atenție suplimentară aspectelor legate de protecția datelor în cadrul programei facultăților de drept. Astfel, ar crește numărul persoanelor suficient de calificate să acorde reprezentare în instanță.

Consolidarea competenței profesionale ar contribui, de asemenea, la reducerea duratei procedurilor. Lacunele la nivelul acestei competențe reprezintă una dintre barierele întâlnite în calea introducerii unor acțiuni în instanță, potrivit raportului FRA din 2012, Access to justice in Europe: an overview of challenges and opportunities (Accesul la justiție în Europa: o prezentare generală a provocărilor și oportunităților), și constatărilor de pe teren.

„Există foarte puțini avocați în barou care se specializează în protecția datelor.” (avocat, Regatul Unit)

Lipsa consultanței și reprezentării legale specializate și accesibile, procedurile complicate și de durată, precum și costurile aferente pot descuraja victimele încălcării protecției datelor să introducă acțiuni în justiție. Procesele complexe, lipsa de informare și sprijinul nespecializat descurajează, de asemenea, cetățenii și îi împiedică să solicite reparații pentru încălcarea protecției datelor.

Cetățenii din fiecare stat membru al UE pot iniția proceduri judiciare pentru corectarea încălcării protecției datelor. Odată lansate procedurile judiciare, există o serie de rezultate posibile care depind de gravitatea încălcării și de tipul de procedură judiciară inițiată – civilă și administrativă sau penală.

„Ei bine, teoretic, reclamantul poate întotdeauna să depună o plângere pe cont propriu, dar nu aș recomanda nimănui acest lucru. Aș recomanda acest lucru în aceeași măsură în care aș recomanda cuiva să se opereze singur pe creier.” (avocat, Finlanda)

Cercetarea socială de teren indică două tendințe în statele membre ale UE, cu consecințe pentru eficiența procedurilor judiciare. Foarte puține cazuri de protecție a datelor sunt inițiate și, drept urmare, judecătorii nu dispun de competențe și experiență în domeniul protecției datelor cu caracter personal. La rândul ei, această situație conduce la marginalizarea aspectelor legate de protecția datelor, care nu sunt considerate drept o prioritate în ceea ce privește programele de formare și de sensibilizare.

Concluzii

Există o serie de modalități de îmbunătățire a disponibilității și calității căilor de atac de care dispun victimele cazurilor de încălcare a protecției datelor în UE. UE, statele sale membre și autoritățile individuale de protecție a datelor au fiecare un rol de jucat în dezvoltarea abordării actuale privind asigurarea unor căi de atac.

Rolul instituțiilor UE este deosebit de important în acest domeniu. Comisia Europeană a propus un proiect de regulament prin care stabilește cadrul general al UE pentru protecția datelor. Cadrul propus vizează armonizarea legislației privind protecția datelor în statele membre ale UE și consolidarea capacității autorităților naționale de protecție a datelor în ceea ce privește corectarea încălcărilor. Este esențial ca autoritățile de protecție a datelor să fie independente de controlul extern, atât în ceea ce privește alocarea și cheltuirea fondurilor, cât și în ceea ce privește recrutarea personalului. O astfel de independență este deosebit de importantă întrucât autoritățile de protecție a datelor trebuie să abordeze și cazurile de încălcare a protecției datelor de către stat. În plus, acestea trebuie să dispună de proceduri adecvate, de competențe suficiente și de resurse corespunzătoare, inclusiv de specialiști calificați care să utilizeze aceste proceduri și competențe.

UE ar trebui să își fixeze obiectivul de a spori finanțarea acordată organizațiilor societății civile și organismelor independente în măsură să ajute victimele care solicită reparații în domeniul protecției datelor. Pentru a consolida capacitatea victimelor de a introduce acțiuni în justiție, UE ar trebui să ia în considerare o mai mare relaxare a normelor privind calitatea procesuală, pentru a permite organizațiilor care acționează în interes public să înainteze plângeri și să deschidă calea către acțiuni colective.

Statele membre ale UE pot contribui la îmbunătățirea mecanismelor existente de protecție a datelor prin luarea de măsuri necesare pentru a spori sensibilizarea publicului larg cu privire la existența și funcționarea mecanismelor disponibile privind introducerea de plângeri pentru încălcarea protecției datelor, precum și cu privire la organizațiile societății civile care oferă sprijin reclamantilor. Statele membre ale UE ar trebui, de asemenea, să ia măsuri pentru consolidarea competențelor profesionale ale judecătorilor și avocaților în domeniul protecției datelor, punând la dispoziție sesiuni de formare și acordând o atenție suplimentară aspectelor legate de protecția datelor în cadrul programelor facultăților de drept. Pe lângă asigurarea calității și a accesului la reprezentarea legală, acest fapt ar contribui la reducerea duratei procedurilor, care a fost subliniată, în cadrul cercetării de teren, ca o barieră în calea celor care doresc să recurgă la căi de atac.

În peisajul drepturilor fundamentale ale UE, autoritățile de protecție a datelor sunt, de asemenea, o componentă importantă și este esențial ca cei care recurg la căi de atac să le recunoască ca atare. Autoritățile de protecție a datelor ar trebui să se axeze pe sensibilizarea cu privire la existența și rolul lor, cultivându-și profilul public în calitate de gardieni independenți ai dreptului fundamental la protecția datelor. De asemenea, acestea ar trebui să aibă în vedere o cooperare mai strânsă cu alți gardieni ai drepturilor fundamentale, precum organismele de promovare a egalității, instituțiile privind drepturile omului și organizațiile societății civile.



Raportul integral *Access to data protection remedies in EU Member States* (Accesul la căile de atac în domeniul protecției datelor în statele membre ale UE) analizează natura încălcării protecției datelor și subliniază obstacolele cu care se confruntă victimele unor astfel de încălcări atunci când solicită reparații. Acest proiect socio-juridic al FRA, care analizează regimurile de protecție a datelor în cele 28 de state membre ale UE și interviurile cu părțile relevante din 16 state membre, subliniază provocările cu care se confruntă cetățenii atunci când recurg la căi de atac. Constatările oferă dovezi pentru informarea Comisiei Europene și pentru a contribui la eforturile acesteia de a reforma și a consolida în mod cuprinzător regimul protecției datelor în UE.

Informații suplimentare:

Pentru raportul integral al FRA *Access to data protection remedies in EU Member States* (Accesul la căile de atac în domeniul protecției datelor în statele membre ale UE), a se vedea: <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states>

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

Prezentul rezumat este disponibil în limbile engleză, franceză și germană. De asemenea, în 2014 se vor publica traduceri și în alte limbi, inclusiv în bulgară, spaniolă, cehă, daneză, estonă, greacă, croată, italiană, letonă, lituaniană, maghiară, neerlandeză, polonă, portugheză, slovacă, slovenă, finlandeză și suedeză.



Oficiul pentru Publicații

FRA – AGENȚIA PENTRU DREPTURI FUNDAMENTALE A UNIUNII EUROPENE

Schwarzenbergplatz 11 – 1040 Viena – Austria
tel. +43 158030-0 – fax +43 158030-699
fra.europa.eu – info@fra.europa.eu
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)
twitter.com/EURightsAgency



© Agenția pentru Drepturi Fundamentale
a Uniunii Europene, 2013
Foto: © SXC

TK-01-13-752-RO-C
doi:10.2811/64974