Nadzor obavještajnih službi: mjere za zaštitu temeljnih prava i pravni lijekovi u Europskoj uniji

Sažetak

Člankom 7. Povelje Europske unije o temeljnim pravima svim pojedincima u Europskoj uniji (EU) jamči se pravo na poštivanje njihovog privatnog i obiteljskog života, dok se člankom 8. jamči pravo na zaštitu njihovih osobnih podataka. Zahtijeva se da se takvi podaci obrađuju pravedno za određene svrhe i svakoj se osobi osigurava pravo na pristup svojim osobnim podacima, kao i pravo da se takvi podaci isprave. Također se određuje da neovisno tijelo mora regulirati poštivanje tog prava. Člankom 47. osigurava se pravo na djelotvorni pravni lijek, uključujući pravično i javno suđenje u razumnom roku.

Kad su mediji diljem svijeta počeli objavljivati „Snowdenove dokumente" u lipnju 2013. godine, javnost je upoznata s postojanjem opsežnih programa globalnog nadzora koje su provodile obavještajne službe. Snowdenove objave nisu prvi slučaj spominjanja programa za nadzor komunikacija širokog razmjera uspostavljenih nakon terorističkih napada na Sjedinjene Američke Države 11. rujna 2001. godine. Međutim, opseg tih objava i dalje je bez presedana i ona su utjecala na privatnost ljudi diljem svijeta. Nadzor više nije samo usmjeren na državne ili poslovne tajne, već omogućuje presretanje komunikacija između velikog broja osoba na globalnoj razini. Time se narušavaju poštivanje privatnog i obiteljskog života pojedinaca i pravo na privatnost i zaštitu osobnih podataka – prava zaštićena na razini Europske unije Poveljom Europske unije o temeljnim pravima svim pojedincima u Europskoj uniji (u daljnjem tekstu: Povelja). Stoga EU i njezine države članice imaju obvezu štititi navedena prava, što se odnosi i na kontekst nadzora, i pružiti žrtvama pravne lijekove radi suočavanja s nezakonitim nadzorom.

„Takav masovni, neselektivni nadzor inherentno je nerazmjeran i predstavlja neopravdano miješanje u prava zajamčena člancima 7. i 8. Povelje."
(CJEU, C-362/14, *Maximillian Schrems protiv povjerenika za zaštitu podataka, mišljenje nezavisnog odvjetnika, 23. rujna 2015.*)

Objave su uzrokovale niz reakcija. Obavještajna zajednica, a osobito tijela nadležna za nadzor obavještajnih službi, temeljito je istražila i proučila smisao i implikacije Snowdenovih objava kroz namjenske istrage i posebna izvješća. Institucije EU-a snažno su reagirale. Europska komisija, Vijeće Europske unije i Europski parlament izvijestili su o objavama i izrazili zabrinutost zbog programa masovnog nadzora, tražili objašnjenje od vlasti Sjedinjenih Američkih Država i radili na „obnovi povjerenja" u odnosima između SAD-a i EU-a. Iako je prerano za procjenu punog učinka Snowdenovih objava, zaključci istraga provedenih u nekim državama članicama EU-a nakon objava istaknuli su potrebu za reformiranjem njihovog trenutnog nacionalnog zakonskog okvira. To je dodatno naglašeno Rezolucijom Europskog parlamenta iz ožujka 2014. o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima [2013/2188(INI), P7_TA (2014)0230] kojom je pokrenut *Europski digitalni Habeas Corpus*.

„Snowdenove objave dale su nam priliku reagirati. Nadam se da ćemo pretvoriti te reakcije u nešto pozitivno što će se nastaviti u sljedećem mandatu ovog Parlamenta, zakon o zaštiti podataka kojim se svi možemo ponositi."
(Claude Moraes, zastupnik u Europskom parlamentu, izvjestitelj u istrazi Europskog parlamenta o programu nadzora Agencije za nacionalnu sigurnost SAD-a, Izjava za medije, 12. ožujka 2014.)

Mapiranje zakonskih okvira država članica EU-a u vezi s nadzorom

U travnju 2014. godine Europski parlament zatražio je od Agencije Europske unije za temeljna prava (FRA) „da provede detaljno istraživanje zaštite temeljnih prava u kontekstu nadzora". FRA je to i učinila mapirajući zakonske okvire 28 država članica EU-a koji se odnose na nadzor i pružanjem pregleda postojećih standarda temeljnih prava. Istraživanje je bilo usmjereno na mehanizme nadzora i pravne lijekove dostupne pojedincima koji navode kršenje prava na privatnost.

Pravnim istraživanjima FRA-e ne ispituju se tehnike nadzora kao takve, već se ocjenjuje kako trenutni zakonski okviri omogućuju primjenu navedenih tehnika i istražuje ključna uloga specijaliziranih tijela u nadzoru rada obavještajnih službi. Osim toga, podrobno se provjerava u kojoj mjeri relevantne mjere štite privatnost i podatke u svakoj od 28 država članica EU-a.

„Obavještajne službe" imaju ovlaštenje djelovati u inozemstvu i usredotočene su na vanjske prijetnje, dok „službe sigurnosti" imaju ovlaštenje djelovati u tuzemstvu i usredotočene su na unutarnje prijetnje. Izraz „obavještajne službe" upotrebljava se u Izvješću FRA-e kao zajednički naziv za obje navedene službe.

Ovaj sažetak predstavlja glavne rezultate istraživanja FRA-e objavljene u cijelosti u izvješću *Nadzor obavještajnih službi: mjere zaštite temeljnih prava i pravnih lijekova u EU - mapiranje zakonskih okvira država članica* (vidjeti Dodatne informacije).

Prikupljanje podataka i obuhvaćenost

Za potrebe ovog istraživanja, FRA je ispitala zakonske okvire nadzora u 28 država članica EU-a, analizirala zakone i relevantne standarde temeljnih prava kako bi predstavila usporednu analizu pravnog konteksta nadzora diljem EU-a.

Na temelju odgovora dobivenih uporabom sustava Franet, višedisciplinarne istraživačke mreže, FRA je sekundarnim („*desk*") istraživanjem prikupila podatke i informacije iz svih 28 država članica EU-a.

Dodatne informacije prikupljene razmjenom s ključnim partnerima kao što su nacionalni časnici za vezu Agencije Europske unije za temeljna prava u državama članicama, specijalizirana tijela i pojedini stručnjaci. Rezultati istraživanja također su uzeli u obzir postojeća izvješća i publikacije kojima je cilj podupiranje nacionalnih zakonodavaca pri postavljanju zakonskih okvira za obavještajne službe i demokratski nadzor istih.

Drugo društveno-pravno izvješće s mišljenjima FRA-e, dobiveno temeljem empirijskog istraživanja, objavit će se u kasnijoj fazi i sadržavat će više informacija o rezultatima koji su ovdje predstavljeni.

Mjere zaštite temeljnih prava i pravo EU-a

„Prava istina je da uporaba tehnologije za masovni nadzor učinkovito i u potpunosti uklanja pravo na privatnost komunikacije na internetu."
(*Ujedinjeni narodi (UN), posebni izvjestitelj za promicanje i zaštitu ljudskih prava i temeljnih sloboda u borbi protiv terorizma (2014.)*, Četvrto godišnje izvješće podneseno Općoj skupštini, *A/69/397, 23. rujna 2014.*)

Sve države članice EU-a obvezne su držati se minimalnih međunarodnih pravnih standarda ljudskih prava koje su razvili Ujedinjeni narodi (UN) i univerzalno su primjenjivi, kao što je Rezolucija Vijeća za ljudska prava o pravu na privatnost u digitalno doba (dok. A/HRC/28/L.27, 24. ožujka 2015.). Razna stručna i ugovorna tijela UN-a osudila su prakse masovnog nadzora nakon Snowdenovih objava. Minimalni standardi također su okvirno opisani standardima Vijeća Europe, uključujući sudsku praksu Europskog suda za ljudska prava (ESLJP). Osim navedenoga, relevantno je pravo EU-a kako ga tumači Sud Europske unije. Konačno, u područjima gdje su izravno primjenjivi samo ograničeni međunarodni propisi – osim postojećih međunarodnih ljudskih prava – također su važne samoregulacijske mjere i upute, smjernice i priopćenja Europske komisije (tzv. *soft law*).

Izvješće je usmjereno na prava na privatnost i zaštitu osobnih podataka sadržana u člancima 7. i 8. Povelje. Pravo na zaštitu osobnih podataka također je propisano primarnim i sekundarnim pravom EU-a koje osigurava zakonitu i samo u mjeri potrebnoj za ispunjenje opravdanog cilja obradu osobnih podataka, u skladu s područjem primjene,. Ta prava obuhvaćaju sve osobe, bilo da su građani Europske unije ili državljani trećih zemalja. Prema članku 52. stavku 1. Povelje, svako ograničenje tog prava mora biti potrebno i zaista odgovarati ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.

Unatoč postojanju međunarodnih smjernica, ne postoji jedinstveno shvaćanje „nacionalne sigurnosti" na razini cijele Europske unije. Ni zakonodavstvo EU-a ni sudska praksa Suda Europske unije dodatno ne definiraju taj pojam, iako je Sud Europske unije izjavio da se iznimke temeljnih prava moraju tumačiti usko i opravdano.

Takvo nejasno razgraničenje pojma „nacionalne sigurnosti" ima posljedice na primjenjivost prava EU-a. Članak 4. stavak 2. Ugovora o Europskoj uniji propisuje da „nacionalna sigurnost posebice ostaje isključiva odgovornost svake države članice". To ne znači da izuzeće „nacionalne sigurnosti" čini pravo EU-a u potpunosti neprimjenjivim. Institucije EU-a, a posebice Sud Europske unije, mogu procjenjivati tumačenje „nacionalne sigurnosti" na razini država članica i način na koji se provode programi nadzora.

Vrste nadzora: ciljni i neciljni

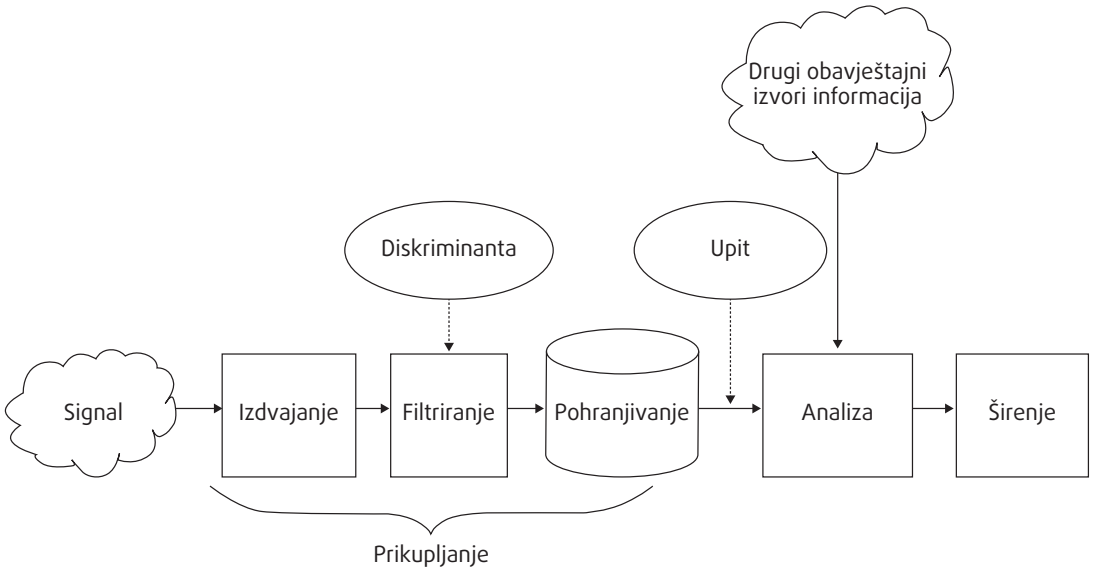
Istraživanjem FRA-e ispituje se kako su organizirani ciljni i neciljni nadzori unutar zakonskih okvira država članica EU-a.

> Nizozemski Neovisni odbor za obavještajne i sigurnosne službe (CTIVD) definira ciljni i neciljni nadzor kako slijedi:
>
> - ciljno presretanje odnosi se na „presretanje pri kojemu se osoba, organizacija ili tehnička značajka koja je cilj prikupljanja podataka može unaprijed odrediti";
> - neciljno presretanje odnosi se na „presretanje pri kojemu se osoba, organizacija ili tehnička značajka koja je cilj prikupljanja podataka ne može unaprijed odrediti".
>
> CTIVD, *Godišnje izvješće 2013.–2014.*, Haag, 31. ožujka 2014. godine, str. 45.–46.

Golem razmjer podataka prikupljenih s pomoću otkrivenih programa nadzora – kao što su PRISM, Xkeyscore i Upstream – potaknuo je dalekosežne reakcije. „Masovni nadzor" (koji se često smatra neciljnim) uključuje prikupljanje znatno drugačijih količina podataka od tradicionalnih, tajnih (ciljnih) postupaka nadzora, kao što je prisluškivanje telefona. Potonji se temelji na prethodnoj sumnji u određenog pojedinca ili organizaciju. Ta vrsta nadzora prevladava u i priznana je zakonima država članica Europske unije. Velika većina zakonskih okvira država članica EU-a ne propisuje ili čak ne spominje „masovni nadzor" kao takav. Samo nekoliko država članica EU-a ima podrobne propise o signalnoj obavještajnoj djelatnosti (SIGINT), što je generički pojam koji se upotrebljava za presretanje signala iz različitih izvora koji obavještajne službe odašilju. Istraživanje FRA-e u svojoj analizi upotrebljava pojam signalne obavještajne djelatnosti.

SIGINT potječe iz vojne obavještajne službe. Odnosi se na automatizirano prikupljanje informacija s pomoću presretanja i prikupljanja digitalnih podataka vezanih za obavještajne aktivnosti. Na slici je istaknuto kako se prikupljeni signali filtriraju s pomoću diskriminanta ili selektora – skupova parametara postavljenih tijekom postupka filtriranja, *a priori* ili dinamički, radi definiranja kriterija kojima se određuju podaci za pohranjivanje kako bi se dobile relevantne informacije (primjerice „sve adrese e-pošte koje se rabe u komunikaciji s Jemenom").

Slika: Konceptualni model signalne obavještajne djelatnosti.



Izvor: Sjedinjene Američke Države, Nacionalno istraživačko vijeće (2015.), str. 28.

Nacionalno istraživačko vijeće Nacionalnih akademija Sjedinjenih Američkih Država upotrebljava pojam signalne obavještajne djelatnosti kao sveobuhvatni pojam za sve podatke pohranjene na elektroničkim uređajima. Venecijanska komisija upotrebljava SIGINT kao zbirni pojam za sredstva i postupke presretanja i analize komunikacija koje se prenose s pomoću radijskih (uključujući satelite i mobilne telefone) i kabelskih tehnologija.

Analiza zakonskih okvira koji reguliraju postupke nadzora obavještajnih službi pokazala je da zakoni pet država članica EU-a (Francuske, Njemačke, Nizozemske, Švedske i Ujedinjenog Kraljevstva Velike Britanije i Sjeverne Irske) podrobno propisuju uvjete koji omogućuju primjenu ciljnog i neciljnog nadzora, kao što je signalna obavještajna djelatnost. Zakoni ostalih država članica nedovoljno određuju navedene uvjete, čime se ometa pravna analiza propisanih postupaka za prikupljanje informacija s pomoću signalne obavještajne djelatnosti. Iako zakoni u tim državama ne određuju SIGINT izravno, on se ipak može provesti. Međutim, s obzirom na to da je navedena praksa propisana samo u neobjavljenim regulatornim mjerama u tim državama, analiza primjenjivih zakonskih okvira neće znatno pojasniti njezinu uporabu.

Ključni rezultati

Obavještajne službe i zakoni o nadzoru

Cilj i struktura obavještajnih službi

Glavni je cilj obavještajnih službi u demokratskim društvima zaštita nacionalne sigurnosti i temeljnih vrijednosti otvorenog društva s pomoću tajnih obavještajnih alata. Ustrojstvo obavještajnih zajednica u pojedinim državama članicama EU-a tijesno je povezano s povijesnim zbivanjima u pojedinim državama i ne drži se nužno standarda temeljnih prava. Kao rezultat toga, obavještajne službe diljem Europske unije uspostavljene su na vrlo različite načine. U nekim državama članicama EU-a obavještajne djelatnosti obavljaju dvije obavještajne službe, dok je u drugim državama za iste djelatnosti nadležno pet ili šest tijela.

- Gotovo sve države članice EU-a imaju najmanje dva različita tijela obavještajnih službi, jedno za civilna i jedno za vojna pitanja; potonja nisu pokrivena ovim izvješćem. Za civilne obavještajne službe uglavnom je nadležno

ministarstvo unutarnjih poslova, a katkad i premijer ili predsjednik.

- U nekim državama članicama civilne obavještajne službe se dalje dijele na jednu službu s ovlastima za djelovanje u tuzemstvu i jednu službu s ovlastima za djelovanje u inozemstvu. Štoviše, neke države članice povjerile su provedbu obavještajnih mjera jedinicama koje su specijalizirane za određene prijetnje poput organiziranog kriminala, korupcije i borbe protiv terorizma.

Zaštita nacionalne sigurnosti

Istraživanjem FRA-e ispituje se pojam „nacionalne sigurnosti" u kontekstu ovlasti obavještajnih službi i mjera nadzora koje one mogu provoditi. Rezultati opet otkrivaju veliku raznolikost među državama članicama EU-a.

- Primarni cilj obavještajnih službi je zaštita nacionalne sigurnosti, ali značenje tog pojma nije usklađeno među svim državama članicama Europske unije. Područje primjene nacionalne sigurnosti malo je gdje definirano, a katkad se upotrebljavaju i slični pojmovi. Druge države članice uopće ne upotrebljavaju pojam „nacionalne sigurnosti", već definiraju „unutarnju sigurnost" i/ili „vanjsku sigurnost" ili „sigurnost države".

- Područje primjene različitih zadaća obavještajnih službi (odnosno, njihove ovlasti) nije istovjetan diljem država članica Europske unije. Osim tradicionalnih područja, ovlasti nekih obavještajnih službi obuhvaćaju pitanja organiziranog kriminala i digitalnog (*cyber*) kriminala. Navedeni pojmovi nisu usklađeno definirani.

Zakonska regulativa nadzora

Granica između zaduženja tijela za provedbu zakona i tijela obavještajnih službi katkad je nejasna. Svako proširenje zadaća mora biti propisno opravdano u mjeri potrebnoj za zaštitu države, što je temeljni razlog za uspostavu obavještajne službe.

- Većina zakonskih okvira država članica EU-a regulira samo ciljni nadzor pojedinaca ili određenih skupina/organizacija. Osim ciljnog nadzora, pet država članica usvojilo je podrobne zakone o uvjetima uporabe signalne obavještajne djelatnosti.

- Uzevši u obzir standarde zaštite temeljnih ljudskih prava koji su na snazi, nacionalnim zakonskim okvirima nedostaje jasna definicija kategorija osoba i područja primjene aktivnosti koje bi mogle biti predmetom obavještajnih radnji.

- Obavještajne službe zakonski su regulirane u većini država članica EU-a (26 od 28). Ustrojstvo i funkcioniranje državnih obavještajnih službi regulirani su zakonskim odredbama. Ustav jedne od država članica zabranjuje obavještajnoj službi obavljanje radnje nadzora. Druga država članica je u postupku donošenja zakona koji će regulirati prakse nadzora svojih obavještajnih službi.

- Analiza FRA-e pokazuje kako se pravni temelj koji uokviruje mandate i ovlasti nacionalnih obavještajnih službi u državama članicama EU-a može sastojati od najmanje jednoga jedinstvenog zakonskog akta kojim se uređuju ustrojstvo i djelatnosti nacionalnih službi, pa do složenih okvira koji se sastoje od nekoliko zakona i pravilnika koji reguliraju određene aspekte ovlasti, ustrojstva, nadležnosti i sredstava.

- Većina država članica organiziralo je rad obavještajnih službi s pomoću dva zakona: jedan koji propisuje ovlasti i ustrojstvo službi, te drugi koji propisuje sredstva djelovanja i uvjete za njihovu primjenu.

- Većina država članica EU-a (23 od ukupno 28) odvojilo je obavještajne službe od tijela za provedbu zakona. Dvije države članice su nedavno ukinule sustave pod kojima su obavještajne službe pripadale policiji ili sličnim tijelima za provedbu zakona.

Nadzor obavještajnih službi

Analiza FRA-e promatra mehanizme odgovornosti u vezi s nadzorom koji provode obavještajne službe. Ona posebno opisuje načine na koje su države članice EU-a uspostavile mehanizme nadzora. Nadzor je sredstvo kojim se osigurava javna odgovornost za odluke i djelovanja obavještajnih službi. Prema riječima stručnjaka nadzorom se nastoji izbjeći zloporaba ovlasti, ozakoniti vršenje nametljivih ovlaštenih postupaka i postići bolji rezultat nakon procjene određenih radnji. Prema općem konsenzusu, preuzetome iz Izvješća Venecijanske komisije i drugih akademskih istraživanja, nadzor bi trebao biti kombinacija:

- izvršne kontrole;
- parlamentarnog nadzora;
- stručnih tijela;
- sudske provjere.

Izvršna kontrola i koordinacija između tijela za nadzor

Izvršna vlast može nadzirati obavještajne službe na različite načine: određivanjem njihovih strateških politika i prioriteta, odnosno utvrđivanjem smjernica; predlaganjem i/ili imenovanjem višega upravnog tijela službi; utvrđivanjem proračuna oko kojeg će parlament u konačnici glasovati; ili odobravanjem suradnje s drugim službama. Izvršna vlast također ima ključnu ulogu u odobravanju mjera nadzora u nekim državama članicama EU-a.

Učinkovit nadzor zahtijeva ispravnu koordinaciju između različitih tijela za nadzor kako bi se osiguralo da se pokriva svaki aspekt rada obavještajnih službi. Ako tijela za nadzor nemaju jasan, cjelovit uvid u rad cjelokupne nacionalne obavještajne zajednice, uslijedit će praznine u nadzoru i učinkovitost nadzornog sustava u cjelini bit će narušena.

- Raznolikost među državama članicama EU-a u pogledu politike i pravnih sustava rezultirala je velikim brojem tijela koja nadziru rad obavještajnih službi. Države članice EU-a imaju znatno različite sustave nadzora. Iako se iz postojećih sustava mogu izvući dobre prakse, pojedina područja mogu imati koristi od zakonskih reformi kojima se povećavaju ovlasti tijela za nadzor.

- Raznim tijelima za nadzor dodijeljen je širok raspon ovlasti koje mogu primjenjivati na različite načine.

- Sedam država članica ima sustave za nadzor koji sjedinjuju izvršnu, parlamentarnu i sudsku vlast (putem *ex ante* odobrenja) i stručna tijela. Međutim, među njima se ne nalaze države sa zakonskim okvirima koji omogućuju prikupljanje informacija s pomoću signalnih obavještajnih djelatnosti.

- Učinkovit nadzor ne zahtijeva nužno primjenu svih četiriju vrsta mehanizama nadzora. Takav se nadzor može postići sve dok se nadležna tijela međusobno dopunjuju i kao cjelina čine snažan sustav sposoban za procjenu ispravnosti provođenja ovlasti obavještajnih službi. To je moguće ako ovlasti nadzora pokrivaju sva područja djelovanja obavještajne službe. Ako su, pak, ovlasti nejasno ili nedovoljno razvijene, tijela za nadzor neće imati željeni utjecaj.

- Izrazito je važno regulirati pristup tijela za nadzor informacijama i dokumentima. Dok su informacije koje prikupljaju obavještajne službe osjetljive naravi i postoje zaštitne mjere kojima se jamči odgovarajuće i pravilno postupanje s njima, tijela za nadzor ne mogu obavljati svoje zadaće bez prethodnog pristupa svim relevantnim informacijama. Čini se kako je suprotno, međutim, norma.

Parlamentarni nadzor

Parlamentarni nadzor ima veliku važnost zbog odgovornosti koju vlada države ima prema tom tijelu. Parlament, kao zakonodavno tijelo, je odgovoran za donošenje jasnih i dostupnih zakonskih propisa kojima se utvrđuju obavještajne službe i određuje njihovo ustrojstvo, posebne ovlasti i ograničenja. Također je nadležan za odobravanje proračuna obavještajnih službi, a u nekim državama članicama provjerava jesu li njihovi postupci u skladu sa zakonskim okvirom.

- Rezultati analize FRA-e pokazuju da 24 države članice EU-a imaju parlamentarni nadzor; u 21 državi članici postoje posebni parlamentarni odbori koji prate rad obavještajnih službi. Neke države članice imaju jedan parlamentarni odbor za nadzor raznih sigurnosnih i obavještajnih službi, dok su druge uspostavile razne odbore za nadzor pojedinih službi.

- Nijedan parlamentarni odbor države članice EU-a nema neograničen pristup obavještajnim podacima.

- Različiti parlamentarni odbori u državama članicama imaju različite ovlasti: većina ima ovlasti za tradicionalni nadzor zakonodavstva, proračuna i prijma informacija o radu obavještajnih službi, dok samo nekolicina može podnositi pritužbe, donositi obvezujuće odluke o obavještajnim službama ili pružati podršku pri odobravanju mjera nadzora.

- U pogledu ovlasti parlamentarnih odbora za pokretanje istraga, zakoni većine država ovlašćuju te odbore da traže informacije od obavještajnih službi ili izvršne vlasti, ali ne da ih i zahtijevaju.

Stručni nadzor

Stručni nadzor izvanredno je vrijedan jer omogućuje pojedincima upoznatima s predmetom, koji imaju vremena posvetiti mu se i neovisni su o političkoj pripadnosti da provjeravaju rad obavještajnih službi. Prema povjereniku za ljudska prava Vijeća Europe, takve osobe često su najpoželjnije na položajima koji im omogućuju svakodnevni nadzor rada sigurnosnih i obavještajnih službi.

- Iako parlamentarni nadzor ima presudnu važnost, on mora biti dopunjen drugim tijelima za nadzor, osobito jakim stručnim tijelima koja mogu pratiti operativne aktivnosti, uključujući prikupljanje, razmjenu i uporabu osobnih podataka, kao i zaštitu prava na privatni život.

- Diljem Europske unije 15 država članica uspostavilo je jedno ili više stručnih tijela posvećenih samo nadzoru obavještajnih službi. Njihove nadležnosti uključuju odobravanje mjera nadzora, istraživanje pritužbi, traženje dokumenata i informacija od obavještajnih službi i davanje savjeta tijelima izvršne i/ili parlamentarne vlasti. Kako bi ostvarila svoj najveći potencijal, stručnim tijelima moraju biti odobreni odgovarajuća neovisnost, resursi i ovlasti.

- U nekim državama članicama EU-a odobravanje mjera nadzora ne uključuje nikakve institucije koje su neovisne o obavještajnim službama i izvršnoj vlasti.

- U državama članicama koje imaju neovisno tijelo zaduženo za odobravanje mjera nadzora ciljni nadzor obično zahtijeva sudsko odobrenje, dok je odobrenje stručnih tijela tek drugo moguće rješenje. Ne postoji zajednički pristup nadzoru signalnih obavještajnih djelatnosti.

- Iako je nužno razumijevanje pravnih aspekata nadzora, stručna tijela također moraju biti tehnički osposobljena. Neke države članice osiguravaju tehničku osposobljenost tijela uključivanjem stručnjaka iz raznih područja znanosti, uključujući informacijske i komunikacijske tehnologije (ICT). Druge se oslanjaju na kombinaciju trenutnih ili bivših sudaca i parlamentaraca.

U državama članicama EU-a tijela za zaštitu podataka (DPA) – tijela specijalizirana za zaštitu privatnosti i podataka – imaju temeljnu ulogu u zaštiti osobnih podataka. Ta je uloga utvrđena je primarnim i sekundarnim pravom EU-a. Međutim, stručna tijela specijalizirana za nadzor obavještajnih službi nesumnjivo su stručna u zaštiti privatnosti i podataka u području obavještajnih djelatnosti.

- Rezultati analize FRA-e pokazuju da, u usporedbi s drugim djelatnostima obrade podataka i upraviteljima podataka iz javnog i privatnog sektora, tijela za zaštitu podataka iz sedam država članica EU-a imaju iste ovlasti nad obavještajnim službama kao i nad svim drugim upraviteljima podataka. Tijela za zaštitu podataka nemaju nikakvu nadležnost nad obavještajnim službama u 12 država članica, a u devet država članica njihove su ovlasti ograničene.

- U državama članicama u kojima tijela za zaštitu podataka dijele nadležnost s drugim stručnim tijelima za nadzor nedostatak međusobne suradnje može uzrokovati praznine koje proizlaze iz fragmentiranih odgovornosti. U državama članicama EU-a u kojima tijela za zaštitu podataka nemaju dostatnu nadležnost nad obavještajnim službama, za osiguravanje zaštite privatnosti i osobnih podataka odgovorno je tijelo za nadzor koje provjerava njezino ispravno provođenje.

- Prijašnja istraživanja FRA-e u području dostupnosti pravnih lijekova za zaštitu podataka istaknula su potrebu za poboljšanjem kapaciteta tijela za zaštitu podataka; to je važno s obzirom na ulogu koju navedena tijela mogu imati u nadzoru obavještajnih službi.

Pravni lijekovi

Prema važećim međunarodnim standardima, svatko tko sumnja da je žrtva kršenja prava na zaštitu privatnosti ili osobnih podataka mora imati priliku popraviti takvo stanje. Pravo na djelotvorni pravni lijek – koji omogućuje pojedincima da traže zadovoljštinu za povredu svojih prava – važan je dio pristupa pravdi. Pravni lijek mora biti „djelotvoran" u praksi i u pravu.

Kao što navedeno u prijašnjim izvješćima FRA-e o pristupu pravnim lijekovima za zaštitu osobnih podataka i pristupu pravdi, žrtvama kršenja prava na zaštitu osobnih podataka dostupno je više načina za poboljšanje dostupnosti i kvalitete pravnih lijekova. Nepravosudna tijela imaju važnu ulogu u pružanju lijekova u području nadzora s obzirom na praktične poteškoće s dostupnošću općih sudova. Nepravosudna tijela u 28 država članica Europske unije obuhvaćaju stručna tijela (uključujući tijela za zaštitu podataka), izvršna i parlamentarna tijela, kao i instituciju pravobranitelja. U nekim državama članicama EU-a, broj nepravosudnih tijela s pomoćnom ulogom u području nadzora razmjerno je ohrabrujući, ali se treba promatrati u kontekstu sljedećih rezultata istraživanja.

Složenost krajolika pravnih lijekova ne olakšava provedbu djelotvornih pravnih lijekova niti to čini količina podataka koje prikupljaju obavještajne službe s pomoću signalne obavještajne djelatnosti. Fragmentacija i kategorizacija načina dostupnosti različitih pravnih lijekova otežava njihovo traženje. Zapravo, prikupljeni podaci pokazuju da je od Snowdenovih objava samo ograničen broj slučajeva pokrenutih protiv prakse nadzora dosuđen na nacionalnoj razini.

Obveza informiranja i pravo na pristup informacijama

Pravo na obaviještenost i pravo na pristup informacijama presudno je kako bi se pojedinci upozorili na mjere nadzora i pokrenule popravne mjere. Europski sud za ljudska prava (ESLJP) je, međutim, prihvatio da se ta prava mogu opravdano ograničiti (vidjeti Europski sud za ljudska prava, Klass i dr. protiv Njemačke, br. 5029/71, 6. rujna 1978.). Rezultati istraživanja FRA-e pokazuju da tajnost rada obavještajnih službi uistinu ograničava navedena prava. Drugi čimbenik je sama količina podataka prikupljenih s pomoću signalnih obavještajnih djelatnosti u usporedbi s tradicionalnim oblicima nadzora.

- U osam država članica EU-a zakonom nisu predviđeni obveza obavještavanja i pravo na pristup informacijama; primjenjuju se pravila o povjerljivosti dokumenata ili službenim tajnama. U ostalih 20 država članica zakonodavstvo predviđa obvezu obavještavanja i pravo na pristup informacijama, u nekim slučajevima u određenim rokovima, ali s ograničenjima. Ta ograničenja imaju različite osnove, kao što su nacionalna sigurnost, nacionalni interesi ili same mjere nadzora.

- Samo dvije države članice imaju posebne odredbe o obvezi obavještavanja u kontekstu signalnih obavještajnih djelatnosti: u jednoj pojedinci nisu obaviješteni ako se primijenjeni selektori izravno ne pripisuju tom pojedincu; u drugoj pojedinac nije obaviješten ako se prikupljeni osobni podaci brišu odmah nakon prikupljanja i dalje se ne obrađuju.

- Tijela za nadzor u deset država članica Europske unije, uključujući šest nacionalnih tijela za zaštitu podataka, nadziru ograničenja prava na primanje obavijesti i prava na pristup informacijama povjeravanjem opravdanosti prijetnje za nacionalnu sigurnost i/ili posrednim pozivanjem na pravo pojedinca na pristup informacijama. U potonjem slučaju tijela procjenjuju može li se odobriti pristup podacima i je li odbijanje pristupa u skladu sa zakonom, a također provjeravaju zakonitost obrade podataka. U jednoj državi članici potreban je sudski nalog kojim se potvrđuje da bi obavijest mogla ugroziti istragu ili postoje neki drugi suprotni argumenti.

- Druge dvije države članice ne dopuštaju pristup informacijama kao takvima. Zakon, međutim, propisuje pravo koje ima isti rezultat: pojedinac može od tijela za nadzor zatražiti provjeru jesu li njegovi/njezini osobni podaci podvrgnuti nezakonitom nadzoru.

- U nekim državama članicama, tijelo za nadzor koje posredno sudjeluje u ostvarivanju prava pojedinca da traži pristup osobnim podacima ne potvrđuje niti negira obradu podataka. Odgovori su obično ograničeni na obavijest je li tužba u postupku rješavanja i/ili provjerena.

Pravni lijekovi

Svaka država članica pruža pojedincima priliku ulaganja prigovora na kršenje privatnosti putem sudova, bez obzira na to jesu li uzrok kršenja ciljne ili signalne obavještajne djelatnosti. Sudovi pružaju mogućnosti pojedincima da ulože žalbu na ometanje svoje privatnosti, uključujući izazivanje odluka tijela za nadzor o njihovim tvrdnjama o kršenju privatnosti. Također daju pojedincima priliku tražiti pravne lijekove – uključujući pravne lijekove u području nadzora.

- Međutim, prijašnja istraživanja FRA-e istaknula su nedostatak specijalizacije sudaca u području zaštite podataka kao ozbiljnu prepreku za učinkovito otklanjanje kršenja prava na zaštitu podataka. Taj rezultat istraživanja relevantan je za područje nadzora u kojemu su, uz nužnu tajnost povezanu s obavještajnim djelatnostima, vrlo važne relevantne stručnosti u informacijskim i komunikacijskim tehnologijama ili obavještajnim radnjama.

- Samo su dvije države članice ublažile nedostatak specijalizacija s obzirom na pravne lijekove uključivanjem sudaca/sudova koji posjeduju potrebna znanja kako bi odlučivali o (često) tehničkim pitanjima i koji smiju pristupiti tajnim materijalima.

Nepravosudni lijekovi

Nepravosudne opcije obično su dostupnije pojedincima od pravosudnih mehanizama jer su pravila postupanja manje stroga, jeftinije je ulaganje pritužbi i brži postupak rješavanja. Prethodni dokazi FRA-e potvrđuju navedeno, posebno u kontekstu zaštite osobnih podataka, jer se više pritužbi podnosi nacionalnim tijelima za zaštitu podataka, a samo ih manji broj uđe u sudski postupak. Broj nepravosudnih tijela – osim tijela za zaštitu podataka – koja djeluju u području zaštite podataka vrlo je mali i, stoga, većina nepravosudnih tijela ima samo ograničene ovlasti pružanja pravnih lijekova.

- Tijela za nadzor (uključujući tijela za zaštitu podataka) zadužena za rješavanje pritužbi neovisne su ustanove u velikoj većini država članica.

- Ako izvršno tijelo za nadzor ima ovlasti pružanja pravnih lijekova, postavlja se pitanje neovisnosti kada ono također ima ovlasti traženja nadzora. Parlamentarna i stručna tijela za nadzor imaju neovisnije upravne strukture – ali neovisnost ne jamči djelotvorno pravno sredstvo, osim ako su poduprta s dovoljno znanja. Pri procjenjivanju neovisnosti takvih tijela potrebno je razmotriti način na koji se imenuju članovi tijela za nadzor i njihov položaj u upravnoj hijerarhiji.

- Tijela za zaštitu podataka u 13 država članica EU-a imaju ovlasti ispitivanja pojedinačnih pritužbi i donošenja obvezujućih odluka. Međutim, u tri od navedenih država članica ograničen je pristup datotekama i prostorima. U pet država članica vrijede dodatni zahtjevi – obvezna nazočnost vodeće osobe ili člana tijela za zaštitu podataka tijekom inspekcije na lokaciji obavještajne službe.

- Pet od sedam država članica koje povjeravaju određene ovlasti pružanja pravnog lijeka svojim stručnim tijelima za nadzor (osim tijela za zaštitu podataka) također dopuštaju tim tijelima donošenje obvezujućih odluka. U dva državama članicama EU-a izvršno tijelo za nadzor također ima ovlasti pružanja pravnog lijeka. Parlamentarni odbori u četiri države članice imaju pravo primiti pojedinačne pritužbe, ali samo ih jedan može riješiti donošenjem obvezujuće odluke.

- Institucija pravobranitelja, koja postoji u svih 28 država članica EU-a, uglavnom se više bavi administrativnim propustima nego stvarnim zaslugama nadzora. Samo jedna država članica EU-a daje instituciji pravobranitelja ovlasti pružanja pravnog lijeka kroz relevantan zakon o obavještajnim djelatnostima. Osim toga, ovlasti institucije pravobranitelja mogu biti vrlo ograničene i postupci obično završavaju neobvezujućim preporukama kojima je cilj ispraviti netočnosti i usmjeriti buduće djelovanje, a ne obvezujućom, izvršnom presudom. To očito utječe na učinkovitost pravnih lijekova koje je u mogućnosti pružiti.

- Ostali elementi koji mogu olakšati pristup pojedinca pravnim lijekovima obuhvaćaju opuštenija pravila o teretu dokaza i tužbe, kao i učinkovitu zaštitu zviždača. Parlamentarna skupština Vijeća Europe smatra zviždanje najučinkovitijim alatom za utvrđivanje granica nadzora.

Zaključci

Baveći se područjem ograničene nadležnosti Europske unije, izvješće naglašava različitost među državama članicama EU-a s obzirom na ustrojstvo obavještajnih službi i načine na koje obavljaju svoje osnovne zadaće.

Mjere nadzora uvelike utječu na prava pojedinaca. S obzirom na njihovu tajnost, pojedinci su dužni prihvatiti određenu razinu povjerenja u tijela javne vlasti koja su, zauzvrat, dužna štititi temeljna prava pojedinaca. Postizanje odgovarajuće razine povjerenja koje svako društvo treba imati prema svojoj obavještajnoj službi zahtijeva odgovornost. Jasno i pristupačno zakonodavstvo, snažni mehanizmi nadzora, odgovarajući mehanizmi kontrole i učinkoviti pravni lijekovi samo su neki od nužnih elemenata za postizanje te vrste odgovornosti, što je i dalje nedvojbeno teško zbog tajnosti rada obavještajnih službi. Uvođenje i održavanje jasnog i pristupačnog zakonodavstva i jakih mehanizama nadzora na razini država članica EU-a predstavlja samo prvi korak prema transparentnom sustavu koji prihvaća i poštuje temeljna prava osoba – teškoće u postizanju navedenoga upućuju na postojanje zapreka.

Reakcije na Snowdenove objave naglasile su potrebu za prilagođivanjem i jačanjem relevantnih zakonskih okvira Europske unije i njezinih država članica. Istraživanja FRA-a pokazuju da je određen broj zakonskih reformi već proveden. Povremene procjene funkcioniranja i legitimnosti okvira koji reguliraju djelatnost obavještajnih službi moraju postati sastavni dio sustava nadzora. Također je temeljno pitanje kako dalje reformirati zakonske okvire za rješavanje nedostatka odgovarajućeg nadzora. Osim toga, reforme koje se provode u državama članicama EU-a trebaju uzeti u obzir tehnološki razvoj kako bi se osiguralo da su mehanizmima nadzora pruženi potrebni alati i stručna znanja. Postizanje navedenoga nedvojbeno je veliki izazov, ali nužan za obavljanje zahtjevne zadaće zaštite sigurnosti uz očuvanje temeljnih prava.

Zaštita javnosti od sigurnosnih prijetnji i zaštita temeljnih prava podrazumijevaju osjetljivu ravnotežu. Teroristički napadi i tehnološke inovacije koje omogućuju praćenje komunikacijskih podataka širokih razmjera dodatno kompliciraju situaciju i izazivaju zabrinutost zbog kršenja prava na privatnost i zaštitu osobnih podataka u ime zaštite nacionalne sigurnosti. Snowdenove objave, koje su otkrile opsežne i nediskriminirajuće nadzorne radnje na globalnoj razini, jasno su istaknule potrebu za poboljšanjem mjera zaštite tih prava.

Ovo izvješće, načinjeno kao odgovor na poziv Europskog parlamenta za provođenjem temeljitog istraživanja o zaštiti temeljnih prava u kontekstu nadzora, mapira i analizira zakonske okvire nadzora u državama članicama EU-a. Usredotočujući se na tzv. „masovni nadzor", izvješće također podrobno opisuje mehanizme nadzora uvedene diljem Europske unije, pruža pregled rada tijela zaduženih za nadzor obavještajnih službi i predstavlja pravne lijekove dostupne pojedincima koji žele osporiti takve obavještajne radnje. Predstavljanjem složenih razmatranja o tim temama, izvješće ističe kako je teško riješiti prioritete koji se često smatraju konkurentnima i pridonosi nastavku rasprave o tome kako ih najbolje pomiriti.

Dodatne informacije:

Za potpuno Izvješće Agencije Europske unije za temeljna prava – *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Nadzor obavještajnih službi: mjere zaštite temeljnih prava i pravnih lijekova u EU – mapiranje pravnih okvira država članica), pogledajte http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services

Pogledajte i druge FRA-ine publikacije iz ovog područja:

- Agencija Europske unije za temeljna prava – Vijeće Europe (2014.), *Priručnik o europskom zakonodavstvu o zaštiti podataka*, Luxembourg, Ured za publikacije, http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law (dostupno na jezicima Europske unije)

- Agencija Europske unije za temeljna prava (2014.), *Access to data protection remedies in EU Member States* (Pristup pravnim lijekovima za zaštitu osobnih podataka u državama članicama EU-a), Luxembourg, Ured za publikacije, http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states i sažetak izvješća http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary (dostupno na jezicima Europske unije)

Pregled aktivnosti Agencije Europske unije za temeljna prava vezanih uz zaštitu osobnih podataka dostupan je na: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Ured za publikacije

FRA – AGENCIJA EUROPSKE UNIJE ZA TEMELJNA PRAVA

Schwarzenbergplatz 11 – 1040 Beč – Austrija
Tel. +43 1580300 – Faks +43 158030699
fra.europa.eu – info@fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

Print: ISBN 978-92-9491-051-6, doi:10.2811/64622
PDF: ISBN 978-92-9491-047-9, doi:10.2811/236486

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