

UDHËZUES I OSBE-SË PËR TRAJNIMIN E
PROFESIONISTËVE TË DREJTËSISË PENALE

Garantimi i respektimit të të drejtave të njeriut në hetimet e krimit kibernetik



Vjenë, tetor 2023
© OSCE 2023

Të gjitha të drejtat e rezervuara. Përmbajtja e këtij publikimi mund të përdoret dhe kopjohet lirisht për qëllime edukuese dhe qëllime të tjera jo-tregtare, me kusht që çdo riprodhim i tillë të shoqërohet me përmendjen e OSBE-së si burimi i informacionit.

ISBN: 978-92-9271-245-7

Publikuar nga:
Secretariati i OSBE-së
Departamenti për Kërcënimet Ndërkombëtare
Njësia e Çështjeve Strategjike të Policisë

Wallnerstrasse 6
1010 Vjenë, Austri
Tel: +43-1 514 36 180
Faksi: +43-1 514 36 105
email: info@osce.org | spmu@osce.org

www.osce.org

UDHËZUES I OSBE-SË PËR TRAJNIMIN

E PROFESIONISTËVE TË DREJTËSISË PENALE

Garantimi i respektimit të të drejtave të njeriut në hetimet e krimit kibernetik

MIRËNJOHJE

Ky udhëzues trajnimi u zhvillua nga Departamenti për Kërcënimet Ndërkombëtare/Njësia e Çështjeve Strategjike të Policisë (TNTD/SPMU) të Sekretariatit të OSBE-së, me të dhëna nga Zyra e OSBE-së për Institucionet Demokratike dhe të Drejtat e Njeriut (ODIHR). TNTD/SPMU-ja dëshiron të falënderojë z. Robert Golobinek dhe z. Hein Dries për kontributin e tyre në hartimin e këtij udhëzuesi. Udhëzuesi u zhvillua në kuadër të projektit të OSBE-së me financim të jashtëm: “Ngritja e kapaciteteve për të luftuar krimin kibernetik në Azinë Qendrore” financiar nga Shtetet e Bashkuara të Amerikës, Gjermania dhe Republika e Koresë.

PËRMBAJTJA

1. Hyrje	05
2. Kuadri ligjor për të drejtat e njeriut që zbatohet në hetimet e krimit kibernetik	09
2.1 Çfarë janë të drejtat e njeriut?	10
2.2 Instrumentet dhe organet ligjore ndërkombëtare të të drejtave të njeriut	10
2.3 Legjislacioni dhe institucionet kombëtare për të drejtat e njeriut	12
3. Të drejtat e njeriut dhe hetimet e krimit kibernetik	15
3.1 Pse janë të rëndësishme të drejtat e njeriut në kontekstin e hetimeve të krimit kibernetik?	16
3.2 Të drejtat e njeriut që preken veçanërisht nga hetimet e krimit kibernetik	17
3.3 Parimet e ligjshmërisë, nevojës dhe proporcionalitetit	20
4. Kompetencat procedurale specifike për krimin kibernetik dhe masat mbrojtëse për të drejtat e njeriut	23
4.1 Veçoritë e hetimeve për krimin kibernetik	24
4.2 Kompetencat procedurale dhe bashkëpunimi ndërkombëtar lidhur me krimin kibernetik	24
4.3 Masat mbrojtëse specifike të të drejtave të njeriut nga krimi kibernetik	26
5. Zbatimi i masave mbrojtëse për të drejtat e njeriut në hetimet e krimit kibernetik	29
5.1 E drejta për privatësi	30
5.2 E drejta për një gjykim të drejtë	37
5.3 E drejta për lirinë e shprehjes	39
5.4 E drejta për mbrojtjen e pronës	42
6. Përfundime	45
7. Shtojcat	47
Shtojca 1 Nenet përkatëse të ICCPR-së dhe KEDNJ-së	48
Shtojca 2 Jurisprudenca e përzgjedhur e GJEDNJ-së	51

AKRONIME

GJDBE	Gjykata e Drejtësisë e Bashkimit Evropian
KE	Këshilli i Evropës
KSBE	Konferenca për Sigurinë dhe Bashkëpunimin në Evropë
KEDNJ	Konventa Evropiane për të Drejtat e Njeriut
GJEDNJ	Gjykata Evropiane për të Drejtat e Njeriut
BE	Bashkimi Evropian
FATF	Task Forca e Veprimit Financiar
GPS	Sistemi i Pozicionimit Global
ICCPR	Pakti Ndërkombëtar për të Drejtat Civile dhe Politike
Adresa IP	Adresa e Protokollit të Internetit
ISP	Ofruesi i Shërbimit të Internetit
OJQ	Organizata Joqeveritare
ODIHR	Zyra për Institucione Demokratike dhe të Drejtat e Njeriut (e OSBE-së)
ZKLDNJ	Zyra e Komisionerit të Lartë të Kombeve të Bashkuara për të Drejtat e Njeriut
OSBE	Organizata për Siguri dhe Bashkëpunim në Evropë
DUDNJ	Deklarata Universale për të Drejtat e Njeriut
OKB	Kombet e Bashkuara
ZKBDK	Zyra e Kombeve të Bashkuara për Drogën dhe Krimin
VPN	Rrjeti Privat Virtual

KUTIZAT ME INFORMACION

KUTIZA 1	Instrumentet juridike ndërkombëtare për të drejtat e njeriut veçanërisht të rëndësishme në hetimet e krimin kibernetik	11
KUTIZA 2	Konventa për krimin kibernetik Neni 15 – Kushtet dhe masat mbrojtëse	26
KUTIZA 3	Instrumentet juridike ndërkombëtare dhe rajonale për mbrojtjen e të dhënave personale	33
KUTIZA 4	Efekti “frenues” mbi lirinë e shprehjes	41

1

Hyrje



Shoqëritë tona po mbështeten gjithnjë e më shumë te teknologjitë digjitale në çdo aspekt të jetës, duke filluar që nga biznesi, shkenca dhe arsimi, tek komunikimi, udhëtimi, çlodhja dhe argëtimi. Zhvillimi i shpejtë i këtyre teknologjive në vitet e fundit ka sjellë shumë mundësi, por edhe rreziqe dhe sfida të reja për sigurinë. Një nga fushat që është ndikuar në mënyrë të konsiderueshme nga këto zhvillime është krimi.

Teknologjitë digjitale kanë shndërruar peizazhin e krimit. Ato kanë krijuar forma të reja të krimit (p.sh., krimi i varur nga kibernetika si softuer me viruse të ndryshme, mashtrimi, vjedhja e kriptomonedhave) dhe kanë ndryshuar mënyrën se si kryhen format ekzistuese të krimit (p.sh., krimi i mundësuar nga kibernetika, si shfrytëzimi seksual në internet ose tregtia në internet në mallra dhe shërbime të paligjshme). Shumë teknologji digjitale janë bërë, gjithashtu, mjete të dobishme për krimet e zakonshme në jetën e përditshme (p.sh., vjedhjet, rrëmbimet dhe mashtrimet). Përveç kësaj, përdorimi i gjerë i pajisjeve digjitale (kompjuterë personalë, laptopë, tableta, telefona celularë, orë inteligjente, etj.) do të thotë se provat digjitale luajnë, tashmë, një rol të rëndësishëm në, pothuajse, të gjitha llojet e hetimeve penale.

Krimi kibernetik ka disa veçori specifike që i bëjnë hetimet e krimeve kibernetike të ndryshme nga hetimet e llojeve të tjera të veprave penale. Veçanërisht, një kriminel nuk ka nevojë të jetë fizikisht i pranishëm në vendin e krimit ose afër një viktime, si dhe mund të ndodhet në një juridiksion të huaj. Për më tepër, interneti ofron shumë mundësi që kriminelët të fshehin identitetin e tyre pas pseudonimeve dhe kredencialeve të vjedhura, si dhe të përdorin mjete të ndryshme të kodimit ose anonimizimit për të fshehur aktivitetin kriminal. Kriptomonedhat i lejojnë përdoruesit të bëjnë pagesa të sigurta pa një lidhje të drejtpërdrejtë me një identitet të botës reale, duke e bërë më të lehtë blerjen e mallrave dhe shërbimeve të paligjshme dhe pastrimin e të ardhurave nga krimi.

Identifikimi, sekuestrimi dhe analizimi i provave digjitale të një krimi kibernetik, ose një lloj tjetër krimi, është gjithashtu i ndryshëm në shumë aspekte nga trajtimi i provave fizike. Provat përkatëse digjitale mund të mos ruhen në një pajisje individuale, por në serverë cloud të kontrolluar nga shoqëritë private, të cilat shpesh i kanë bazat jashtë vendit. Veç kësaj, të dhënat elektronike janë të paqëndrueshme dhe mund të lëvizin, ndryshohen ose fshihen lehtësisht.

Krimi kibernetik¹ dhe provat digjitale paraqesin, si rrjedhojë, sfida të rëndësishme për sistemet e drejtësisë penale dhe sundimin e ligjit në të gjithë rajonin e OSBE-së. Hetimi i krimit kibernetik dhe provave digjitale kërkon njohuri dhe aftësi të veçanta, mjete teknike dhe kuadër ligjor të përshtatshëm, si dhe bashkëpunim ndërkombëtar efektiv dhe efikas me aktorë të huaj të drejtësisë penale dhe subjektet private. Shtetet janë përshtatur me këto zhvillime duke ndryshuar ligjet e tyre, duke ndërtuar kapacitetet e tyre teknike dhe duke vënë në veprim kompetenca të reja hetimore procedurale. Të gjitha këto masa dhe mjete duhet të zhvillohen dhe të përdoren në përputhje me përgjegjësitë e shteteve sipas ligjit ndërkombëtar për të drejtat e njeriut.

Sikurse me çdo hetim tjetër penal, hetimet e krimit kibernetik dhe përdorimi i kompetencave të veçanta procedurale prekin të drejtat dhe liritë e njeriut të përcaktuara në instrumentet ndërkombëtare në nivel global dhe rajonal. Këto përfshijnë Deklaratën Universale të të Drejtave të Njeriut (DUDNJ), Paktin Ndërkombëtar për të Drejtat Civile dhe Politike (ICCPR) dhe Konventën Evropiane për të Drejtat e Njeriut (KEDNJ).

Shënim: Të gjitha burimet elektronike janë aksesuar më 1 qershor 2023.

1 Në këtë tekst, "krimi kibernetik" përdoret si një term i përgjithshëm që i referohet krimeve të varura nga kibernetika dhe krimeve të krijuara nga kibernetika, përveç nëse specifikohet ndryshe.

Ndërsa këto të drejta dhe liri duhet të respektohen dhe mbrohen në çdo hetim penal, kjo nevojë është, ndoshta, edhe më e rëndësishme në kontekstin e krimit kibernetik dhe provave digjitale. Të dhënat që pajisjet digjitale dhe shërbimet online mbledhin për përdoruesit e tyre janë të paprecedentë si për sa i takon fushëveprimin, ashtu edhe vëllimit të tyre. Këto të dhëna mund të japin shumë informacion për jetën e njerëzve, duke përfshirë shëndetin e tyre, aktivitetin ekonomik, marrëdhëniet private dhe preferencat politike. Kur mbledhin prova digjitale gjatë një hetimi, punonjësit e drejtësisë penale shpesh gjejnë prova të përshtatshme krahas sasive të mëdha të të dhënave të tjera, shpesh personale. Si rrjedhojë, ky lloj hetimi është potencialisht shumë më ndërhyrës sesa hetimet e zakonshme "offline" të cilat mbledhin vetëm prova fizike.

Prandaj, ndërgjegjësimi për implikimet e të drejtave të njeriut që sjellin hetimet e krimit kibernetik dhe hetimet e tjera që përfshijnë prova digjitale është i rëndësishëm për hetuesit e policisë, prokurorët dhe gjyqtarët. Shkelja e të drejtave të njeriut gjatë hetimeve dhe procedurave penale mund të çojë në dënime të gabuara, ose në hedhjen poshtë të provave, çka çon në lirimin e autorit. Mungesa e respektimit të të drejtave të njeriut minon, gjithashtu, besimin në nivel kombëtar dhe ndërkombëtar. Është një pengesë për bashkëpunimin ndërkombëtar, si me organet e zbatimit të ligjit dhe autoritetet e tjera në vendet partnere, po ashtu edhe me shoqëritë private që gjenden jashtë vendit. Gjithashtu, respektimi dhe mbrojtja e të drejtave të njeriut në praktikë ndihmon në forcimin e besimit ndërmjet autoriteteve të drejtësisë penale dhe shoqërisë më gjerë dhe, në këtë mënyrë, inkurajon individët të bashkëpunojnë - dhe t'u japin informacion të rëndësishëm - hetuesve të krimit kibernetik. Prandaj, ndjekja e një qasjeje që bazohet tek të drejtat e njeriut rrit efikasitetin e hetimeve të krimit kibernetik.

Ky Udhëzues synon të rrisë ndërgjegjësimin e profesionistëve të drejtësisë penale për implikimet që mund të ketë hetimi i krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale për të drejtat e njeriut dhe t'i mbështesë ata për të mbrojtur të drejtat e njeriut gjatë punës së tyre të përditshme hetimore. Udhëzuesi e bën këtë duke u përqendruar tek të drejtat e njeriut që preken në mënyrë të veçantë nga hetimet e krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale, përkatësisht:

- E drejta për privatësi;
- E drejta për një gjykim të drejtë;
- E drejta për lirinë e shprehjes/fjalës;
- E drejta për mbrojtjen e pronës.

Udhëzuesi bazohet në jurisprudencën e Gjykatës Evropiane për të Drejtat e Njeriut (GJEDNJ) dhe, herë pas here, të Gjykatës së Drejtësisë së Bashkimit Evropian (GJDBE) për të shpjeguar dhe ilustruar se si zbatohen të drejtat e njeriut në kontekstin e hetimeve të krimit kibernetik dhe në mbledhjen dhe përdorimin e provave digjitale.

2

Kuadri ligjor për të drejtat e njeriut që zbatohet në hetimet e krimit kibernetik

- 2.1** ÇFARË JANË TË DREJTAT E NJERIUT?
- 2.2** INSTRUMENTET DHE ORGANET LIGJORE NDËRKOMBËTARE TË TË DREJTAVE TË NJERIUT
- 2.3** LEGJISLACIONI DHE INSTITUCIONET KOMBËTARE PËR TË DREJTAT E NJERIUT

2.1 ÇFARË JANË TË DREJTAT E NJERIUT?

Të drejtat e njeriut janë të drejta ligjore të individëve për mbrojtjen e dinjitetit dhe lirive të tyre. Ato janë themelore për të gjitha qeniet njerëzore, pa dallim race, ngjyre, gjinie, gjuhe, feje, opinioni politik apo çdo lloj opinioni, prejardhje kombëtare ose sociale, statusi pasuror, lindjeje apo ndonjë status tjetër. Të gjitha të drejtat e njeriut, qofshin ato të drejta civile dhe politike (si të drejtat për jetën, barazinë para ligjit dhe lirinë e shprehjes); të drejtat ekonomike, sociale dhe kulturore (si të drejtat për punë, sigurime shoqërore dhe arsim); ose të drejtat kolektive (si të drejtat për zhvillim dhe vetëvendosje) janë të pandashme, të ndërlihdura dhe të ndërvarura. Përmirësimi i njërës së drejtë lehtëson përparimin e të tjerave.

Të drejtat universale të njeriut shprehen dhe garantohen me ligj në formën e traktateve, të drejtës ndërkombëtare zakonore, parimeve të përgjithshme dhe burimeve të tjera të së drejtës ndërkombëtare. E drejta ndërkombëtare për të drejtat e njeriut imponon detyrime specifike për shtetet, duke përfshirë parlamentet, ministritë, autoritetet lokale, autoritetet e zbatimit të ligjit dhe të drejtësisë penale, si "bartësit e detyrës" përgjegjës për respektimin, mbrojtjen dhe përmbushjen e të drejtave të njeriut. Kjo përfshin si detyrimet e ashtuquajtura "negative" për t'u përmbajtur nga disa akte (p.sh., nga ndërhyrja në mënyrë të paligjshme në jetën private të një personi), ashtu edhe përgjegjësinë për të marrë përsipër veprime "pozitive" për të mbrojtur të drejtat e një personi (p.sh., duke hetuar në mënyrë efektive dhe ndjekur penalisht krimet) dhe promovimin e të drejtave dhe lirive themelore të njeriut (p.sh., duke ofruar informacion publik dhe trajnim për zyrtarët përkatës shtetërorë).

2.2 INSTRUMENTET DHE ORGANET JURIDIKE NDËRKOMBËTARE PËR TË DREJTAT E NJERIUT

Shtetet e njohën rëndësinë e mbrojtjes së të drejtave të njeriut pas Luftës së Dytë Botërore me themelimin e Kombeve të Bashkuara (OKB) dhe Këshillit të Evropës (KE) dhe me përpunimin e instrumenteve ndërkombëtare për të drejtat e njeriut në kuadrin e këtyre organizatave. Bashkimi Evropian (BE), gjithashtu, ka vënë në pah rëndësinë e të drejtave të njeriut duke miratuar një kartë të dedikuar për të drejtat e njeriut. Kutiza 1 paraqet instrumentet ligjore ndërkombëtare të të drejtave të njeriut, veçanërisht të rëndësishme në kontekstin e krimit kibernetik.

KUTIZA 1 INSTRUMENTET JURIDIKE NDËRKOMBËTARE PËR TË DREJTAT E NJERIUT VEÇANËRISHT TË RËNDËSISHME NË HETIMET E KRIMIT KIBERNETIK

- Deklarata Universale për të Drejtat e Njeriut e 1948² (DUDNJ) e OKB-së (veçanërisht Nenet 8 - 11, 12 dhe 19);
- Pakti Ndërkombëtar për të Drejtat Civile dhe Politike i 1966³ (ICCPR) i OKB-së (veçanërisht Nenet 14, 17 dhe 19);
- Konventa Evropiane për të Drejtat e Njeriut e 1950⁴ (KEDNJ) e KiE-së (veçanërisht Nenet 6, 8 dhe 10);
- Karta e të Drejtave Themelore të Bashkimit Evropian⁵ e 2000.

Shtojca 1 paraqet tekstin e plotë të neneve të lartpërmendura të ICCPR-së dhe KEDNJ-së.

Me përjashtim të Selisë së Shenjtë, të gjitha shtetet pjesëmarrëse të OSBE-së kanë ratifikuar ICCPR-në dhe për këtë arsye kanë detyrimin ta zbatojnë atë. Shumica e shteteve pjesëmarrëse të OSBE-së janë, gjithashtu, anëtare të KE-së dhe, si rrjedhojë, palë të KEDNJ-së. Disa shtete pjesëmarrëse të OSBE-së janë, gjithashtu, Shtete Anëtare të BE-së dhe për këtë arsye janë të detyruara të respektojnë Kartën e të Drejtave Themelore të Bashkimit Evropian kur zbatojnë ligjin e BE-së (Neni 51, paragrafi 1 i Kartës).

Ka një mori institucionesh për të drejtat e njeriut, të cilat janë të autorizuara të interpretojnë dhe promovojnë të drejtat e njeriut të sanksionuara në këto tekste ligjore. Në nivel të OKB-së, Komiteti i të Drejtave të Njeriut është organi i traktatit të ICCPR-së. Ai përbëhet nga 18 ekspertë të pavarur që monitorojnë zbatimin e ICCPR-së nga Shtetet Palë.⁶ Komiteti shqyrton zbatimin e Paktit nëpërmjet raporteve periodike dhe mund të shqyrtojë ankesat individuale lidhur me shkeljet e pretenduara të ICCPR-së nga shtetet që kanë miratuar Protokollin Opsional të Paktit.⁷

Në nivel rajonal, Gjykata Evropiane për të Drejtat e Njeriut (GJEDNJ) gjykon kërkesat e paraqitura nga individë, grupe individësh, ose një apo më shumë nga shtetet anëtare të KiE-së, të cilët pretendojnë se u janë shkelur të të drejtat e përcaktuara në KEDNJ. Vendimet e GJEDNJ-së janë ligjërisht të detyrueshme për shtetet përkatëse anëtare të KiE-së, por jurisprudenca e saj mund të ofrojë udhëzime të rëndësishme për vendet e tjera lidhur me fushëveprimin dhe zbatimin e të drejtave civile dhe politike. Gjykata e Drejtësisë së Bashkimit Evropian (GJDBE) interpreton ligjin e BE-së, duke përfshirë Kartën e të Drejtave Themelore të Bashkimit Evropian.⁸ Vendimet e saj janë ligjërisht të detyrueshme për shtetet anëtare të BE-së.

2 Deklarata Universale për të Drejtat e Njeriut, 10 dhjetor 1948, Rezoluta e Asamblesë së Përgjithshme të OKB-së 217 A (III).

3 Pakti Ndërkombëtar për të Drejtat Civile dhe Politike, 16 dhjetor 1966, Rezoluta e Asamblesë së Përgjithshme të OKB-së 2200A (XXI), hyrë në fuqi më 23 mars 1976.

4 Konventa për Mbrojtjen e të Drejtave të Njeriut dhe Lirive Themelore, 4 nëntor 1950, CETS Nr. 5, hyrë në fuqi më 3 shtator 1953.

5 Karta e të Drejtave Themelore të Bashkimit Evropian, 18 dhjetor 2000, OJEC 2012/C 326/02, hyrë në fuqi më 1 dhjetor 2009.

6 ZKLDNJ (pa datë), Komiteti për të Drejtat e Njeriut, i disponueshëm në <https://www.ohchr.org/en/treaty-bodies/ccpr>.

7 Protokollin Opsional i Paktit Ndërkombëtar për të Drejtat Civile dhe Politike, 16 dhjetor 1966, Rezoluta e Asamblesë së Përgjithshme të OKB-së 2200A (XXI), hyrë në fuqi më 23 mars 1976.

8 Protokollin 3 mbi Statutin e Gjykatës së Drejtësisë së Bashkimit Evropian, 16 dhjetor 2004, OJEU C 310/210.

Organet e tjera kanë një mandat këshillues për të forcuar promovimin dhe mbrojtjen e të drejtave të njeriut. Në nivel ndërkombëtar, këto përfshijnë Këshillin e OKB-së⁹ për të Drejtat e Njeriut dhe një numër procedurash të posaçme në dispozicion të tij, përfshirë raportuesit specialë, përfaqësuesit specialë, ekspertët e pavarur dhe grupet e punës.¹⁰ Përveç kësaj, Zyra e Komisionerit të Lartë të OKB-së për të Drejtat e Njeriut (ZKLDNj) promovon dhe mbron të gjitha të drejtat e njeriut përmes studimit, edukimit, mbrojtjes dhe ndihmës për qeveritë.

Respektimi i të drejtave dhe lirive themelore të njeriut janë, gjithashtu, kyçe për konceptin e plotë të OSBE-së për sigurinë. Që nga nënshkrimi i Aktit Final të Helsinkit në 1975, Konferenca për Sigurinë dhe Bashkëpunimin në Evropë (KSBE) dhe më pas OSBE-ja kanë zhvilluar një numër të konsiderueshëm angazhimesh në fushat e të drejtave të njeriut, demokracisë, shtetit të së drejtës dhe pakicave kombëtare miratuar nga organe të ndryshme vendimmarrëse të KSBE-së dhe më vonë të OSBE-së.¹¹ Shumë prej këtyre angazhimeve kanë rëndësi për punën e institucioneve të drejtësisë penale, edhe në kontekstin e hetimit dhe ndjekjes penale të krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale. Ndonëse angazhimet e OSBE-së nuk kanë karakterin e traktateve ligjrisht të detyrueshme sipas së drejtës ndërkombëtare, ato përfaqësojnë angazhime të rëndësishme politikisht të detyrueshme, të miratuara me konsensus nga të gjitha shtetet pjesëmarrëse.

2.3 LEGJISLACIONI DHE INSTITUCIONET KOMBËTARE PËR TË DREJTAT E NJERIUT

Për të pasur efekt, standardet ndërkombëtare për të drejtat e njeriut duhet të zbatohen dhe mbrohen nga legjislacioni, politika dhe praktika kombëtare. Është në radhë të parë detyrë e ligjvënësve të marrin masa që kuadri ligjor kombëtar të pasqyrojë dhe inkorporojë standardet ndërkombëtare për të drejtat e njeriut. Zakonisht, mbrojtja e të drejtave të njeriut integrohet në kushtetutat e vendeve dhe në legjislacione të tjera ndërsektoriale ose sektoriale. Të drejtat procedurale inkorporohen, përgjithësisht, në kodet e procedurës penale nëpërmjet kushteve dhe masave të ndryshme mbrojtëse.

Legjislacioni kombëtar për të drejtat e njeriut interpretohet nga gjykatat kombëtare, duke përfshirë gjykatat kushtetuese – kur bëhet fjalë për dispozitat kushtetuese. Tërësia e jurisprudencës kombëtare ofron udhëzime të rëndësishme për zbatimin në praktikë të legjislacionit vendas për të drejtat e njeriut.

Gjithashtu, organet kombëtare për të drejtat e njeriut (si institucionet kombëtare të të drejtave të njeriut, ose Avokati i Popullit) kanë një funksion të rëndësishëm në mbrojtjen e të drejtave të njeriut në nivel kombëtar duke ofruar këshilla dhe duke ndërmarrë veprime në rastet individuale

9 Këshilli i OKB-së për të Drejtat e Njeriut, 15 mars 2006, Rezoluta e Asamblesë së Përgjithshme të OKB-së 60/251, duke zëvendësuar Komisionin e OKB-së për të Drejtat e Njeriut më 16 qershor 2006.

10 Këshilli i OKB-së për të Drejtat e Njeriut (pa datë), *Procedurat e Posaçme të Këshillit për të Drejtat e Njeriut*, të disponueshme në <https://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx>.

11 Për një pasqyrë të përgjithshme, shih OSBE/ODIHR, *Angazhimet e OSBE-së për Dimensionin Njerëzor: Vëllimi 1 - Përmbledhja tematike*, botimi i 4-të (Varshavë, 2023); dhe OSBE/ODIHR, *Angazhimet e OSBE-së për Dimensionin Njerëzor: Vëllimi 2 - Përmbledhja kronologjike*, botimi i 4-të (Varshavë, 2023).

të shkeljeve. Përveç kësaj, shoqëria civile, përfshirë organizatat joqeveritare (OJQ-të) dhe mediat luajnë një rol vendimtar në rritjen e ndërgjegjësimit për të drejtat e njeriut, mbrojtjen e interesave publike dhe promovimin e kontrollit publik për respektimin e të drejtave të njeriut.

3

Të drejtat e njeriut dhe hetimet e krimit kibernetik

- 3.1** PSE JANË TË RËNDËSISHME TË DREJTAT E NJERIUT NË KONTEKSTIN E HETIMEVE TË KRIMIT KIBERNETIK?
- 3.2** TË DREJTAT E NJERIUT QË PREKEN VEÇANËRISHT NGA HETIMET E KRIMIT KIBERNETIK
- 3.3** PARIMET E LIGJSHMËRISË, NEVOJËS DHE PROPORCIONALITETIT

3.1 PSE JANË TË RËNDËSISHME TË DREJTAT E NJERIUT NË KONTEKSTIN E HETIMEVE TË KRIMIT KIBERNETIK?

Aktorët shtetërorë, duke përfshirë ministrinë dhe profesionistët e drejtësisë penale, kanë përgjegjësinë kryesore për të respektuar, mbrojtur dhe përmbushur të drejtat e njeriut. Kjo përfshin garantimin e zbatimit në praktikë të standardeve për të drejtat e njeriut të përfshira në konventat ndërkombëtare në të cilat shteti është palë. Detyrimet e shteteve përfshijnë të gjitha aspektet e reagimit të drejtësisë penale ndaj krimit kibernetik. Ato përfshijnë marrjen e masave që legjislacioni vendas të jetë në përputhje me të drejtat e njeriut dhe të përmbajë garancitë e nevojshme procedurale, ndërgjegjësimin e profesionistëve për përgjegjësinë e tyre për të mbrojtur të drejtat e njeriut, monitorimin e zbatimit të të drejtave të njeriut në praktikë dhe sigurimin e rrugëve ligjore që duhet të ndjekin individët kur u shkelen të drejtat e njeriut.

Përveçse është detyrim sipas ligjit ndërkombëtar, mbrojtja e të drejtave të njeriut ka përfitime të qarta praktike për hetimet e krimit kibernetik dhe punën e autoriteteve të drejtësisë penale, në përgjithësi, siç tregojnë shembujt në vijim.

Së pari, respektimi i të drejtave të njeriut është i rëndësishëm për sigurimin e provave të nevojshme nga jashtë dhe për të mundësuar bashkëpunimin ndërkombëtar ndërmjet autoriteteve të drejtësisë penale dhe me shoqëritë private. Mosrespektimi i standardeve të të drejtave të njeriut, për shembull, mund të jetë një arsye për refuzimin e një kërkesë të ndërsjellë për ndihmë ligjore. Në shumë shtete, kushti paraprak për të ofruar ndihmë zyrtare është që shteti kërkuar të garantojë një gjykim të drejtë dhe të respektojë të drejtat e njeriut të përcaktuara në instrumentet ndërkombëtare dhe rajonale për të drejtat e njeriut. Edhe shoqëritë private, përfshirë ofruesit kryesorë të shërbimeve si Microsoft, Google ose Meta, marrin parasysh të dhënat e të drejtave të njeriut të një shteti kur vendosin se si t'i përgjigjen një kërkesë për ruajtjen ose shpërndarjen e të dhënave për t'u përdorur në një hetim penal.¹²

Së dyti, mosrespektimi i të drejtave të njeriut dhe masave mbrojtëse procedurale gjatë kryerjes së një hetimi mund të bëjë që gjykata t'i konsiderojë provat të papranueshme. Kjo është veçanërisht e rëndësishme në hetimet e krimit kibernetik, të cilat mund të përfshijnë teknika hetimore që lënë gjurmë dhe mbështeten në prova të paqëndrueshme digjitale. Për rrjedhojë, zbatimi i standardeve të të drejtave të njeriut përgjatë gjithë hetimit, rrit mundësitë për një dënim të suksesshëm të autorëve.

Së treti, autoritetet e drejtësisë penale që nuk arrijnë të hetojnë krimin kibernetik sipas standardeve të të drejtave të njeriut mund të bëhen objekt i procedurave të ankimimit ose veprimeve ligjore. Drejtuesit dhe oficerët e policisë, për shembull, mund të përballen si individë me sanksione administrative ose penale, nëse përfshihen në hetime që konstatohet se janë kryer në mënyrë të paligjshme. Kjo mund të shkaktojë një efekt të dëmshëm në moralin dhe reputacionin e autoriteteve, si dhe në mundësinë e dhënies se dënimit për autorët e krimeve kibernetike.

Së fundmi, shkeljet e të drejtave të njeriut gjatë hetimeve të krimit kibernetik mund të çojnë në

12 Shih p.sh., ZKBDK, *Udhëzues praktik për kërkimin e provave digjitale përtej kufijve* (Vjenë, 2021), f. 18, 37.

humbjen e besimit të publikut te autoritetet e drejtësisë penale, duke e bërë më të vështirë arritjen e bashkëpunimit të nevojshëm për të luftuar siç duhet krimin kibernetik. Mungesa e besimit jo vetëm që minon masat për parandalimin e krimit kibernetik, por gjithashtu mund të ndikojë negativisht në gatishmërinë e publikut për të raportuar këto krime ose për të dëshmuar. Prandaj, respektimi dhe mbrojtja e të drejtave të njeriut në kontekstin e hetimeve të krimit kibernetik janë të nevojshme për të siguruar qëndrueshmërinë, efektivitetin dhe, eventualisht, suksesin e përpjekjeve për të luftuar krimin kibernetik.

3.2 TË DREJTAT E NJERIUT QË PREKEN VEÇANËRISHT NGA HETIMET E KRIMIT KIBERNETIK

Hetimet e krimit kibernetik mund të ndikojnë në gëzimin e shumë të drejtave të njeriut. Të drejtat e njeriut në vijim janë veçanërisht të rëndësishme në kontekstin e hetimeve të krimit kibernetik:

- E drejta për privatësi;
- E drejta për gjykim të drejtë;
- E drejta për lirinë e shprehjes/fjalës;
- E drejta për mbrojtjen e pronës.

Teksti i plotë i neneve të ICCPR-së dhe KEDNJ-së që përcaktojnë këto të drejta mund të gjendet në Shtojcën 1.

Të drejta të tjera që mund të preken në mënyrë të drejtpërdrejtë ose të tërthortë nga hetimet e krimit kibernetik përfshijnë: mosdiskriminimin, lirinë e fesë ose besimit, lirinë e organizimit, të drejtën për liri dhe të drejtat e fëmijës.

E DREJTA PËR PRIVATËSI

E drejta për privatësi përcaktohet në Nenin 17 të ICCPR-së dhe Nenin 8 të KEDNJ-së, ku përmendet si e drejta për respektimin e jetës private dhe familjare. Përveç detyrimeve të tyre sipas këtyre instrumenteve, shtetet pjesëmarrëse të OSBE-së janë angazhuar në Dokumentin e Moskës të vitit 1991 për të drejtën e mbrojtjes së jetës private dhe familjare, vendbanimit, korrespondencës dhe komunikimeve elektronike, si dhe për parandalimin e ndërhyrjeve arbitrare në çështjet individuale.¹³

E drejta për privatësi është e domosdoshme në një shoqëri demokratike. Ajo përfshin mbrojtjen e privatësisë së mesazheve, telefonatave dhe email-ve, si dhe mbrojtjen nga mbikëqyrja e paligjshme dhe e panevojshme e shtetit. Për të përmbushur të drejtën e privatësisë, shtetet kanë një detyrim pozitiv (për të mbrojtur të drejtën) dhe një detyrim negativ (të përmbahen nga ndërhyrja në të drejtën). E drejta për privatësi, gjithashtu, u jep mundësi individëve të marrin masa për të mbrojtur

13 OSBE/KSBE, *Dokumenti i Moskës 1991*, 3 tetor 1991, KSBE/CHDM.49/Rishikimi 1, paragrafi 24; OSCE/CSCE, *Dokumenti i Kopenhagës 1990*, 27 qershor 1990, KSBE/CHDC.43, paragrafi 26, shënimi 16.

jetën e tyre private, për shembull, duke përdorur teknologjitë që përmirësojnë privatësinë, si kodimi dhe rrjetet private virtuale (VPN-të).

Për shkak të rëndësisë që ka e drejta për privatësi, ajo është përshkruar si "e drejta e portës". Pa privatësi, gëzimi i plotë i një sërë të drejtash të tjera rrezikohet, për shembull, për të shprehur mendimet, për t'u shoqëruar me të tjerët, ose për të marrë pjesë lirisht në jetën publike dhe politike.¹⁴

Mbrojtja e të dhënave është një pjesë e rëndësishme e së drejtës për privatësi, siç njihet nga Komiteti i OKB-së për të Drejtat e Njeriut¹⁵ dhe GJEDNJ.¹⁶ Një mori instrumentesh ndërkombëtare dhe rajonale përfshijnë parime specifike të mbrojtjes së të dhënave që duhet të respektohen për të garantuar përputhjen e plotë me të drejtën për privatësi.¹⁷ Këto përfshijnë, për shembull, parimet që të dhënat personale, të cilat i nënshtrohen përpunimit automatik të:

- Merren dhe përpunohen në mënyrë të drejtë dhe të ligjshme;
- Ruhen për qëllime të përcaktuara dhe të ligjshme (të kufizohen tek qëllimi);
- Jenë të përshtatshme, të duhurat dhe jo me tepri (minimizimi i të dhënave);
- Ruhen jo më gjatë nga sa kërkohet (mbajtja e kufizuar e të dhënave);
- Mbrohen nga aksesimi i paautorizuar.

Sikurse ndodh me shumë të drejta, e drejta për privatësi nuk është absolute dhe mund të kufizohet në rrethana të caktuara. Çdo ndërhyrje në ushtrimin e kësaj të drejte duhet të **bazohet në ligj**, të **diktohet nga nevoja** në një shoqëri demokratike, si p.sh., për të mbrojtur sigurinë kombëtare ose sigurinë publike, ose për të parandaluar trazira ose krime, dhe të jetë **proporcionale** (shih gjithashtu seksionin 3.3). Për shembull, policia mund të autorizohet nga një autoritet gjyqësor kompetent të përgjojë bisedat e një individi nëse ka shkaqe të arsyeshme për të besuar se individi është gati të kryejë një krim të rëndë.

E DREJTA PËR NJË TË GJYKIM TË DREJTË

E drejta për një gjykim të drejtë është një element thelbësor i mbrojtjes së të drejtave të njeriut dhe shërben si një mjet procedural për të mbrojtur sundimin e ligjit.¹⁸ Si Neni 14 i ICCPR-së, ashtu edhe Neni 6 i KEDNJ-së përcaktojnë një sërë kërkesash të dallueshme që së bashku përbëjnë të drejtën për gjykim të drejtë, duke përfshirë të drejtën që kushdo që akuzohet për një veprë

14 ZKLDNJ (2018), *Deklarata Universale për të Drejtat e Njeriut në 70: 30 Nene për 30 Nene, Neni 12*, i disponueshëm: <https://www.ohchr.org/en/press-releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12>.

15 Shih Komiteti i OKB-së për të Drejtat e Njeriut, *Komenti i Përgjithshëm nr. 16 në Nenin 17, E drejta për privatësi*, 8 prill 1988, Dokumenti i OKB-së HRI/GEN/1/Rishikimi 1, f. 21–23, paragrafi 10.

16 GJEDNJ, *Udhëzues për Nenin 8 të Konventës Evropiane për të Drejtat e Njeriut: E drejta për respektimin e jetës private dhe familjare, shtëpisë dhe korrespondencës* (Strasburg, 2022); shih gjithashtu GJEDNJ (2023), *Fleta e të dhënave për Mbrojtjen e të Dhënave Personale*, e disponueshme në https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

17 Shih, p.sh., *Konventa për Mbrojtjen e Individëve në lidhje me Përpunimin Automatik të të Dhënave Personale*, 28 janar 1981, CETS Nr.108; Karta e të Drejtave Themelore të BE-së, Neni 8 në kombinim me Rregulloren e Përgjithshme të BE-së për Mbrojtjen e të Dhënave, 27 Prill 2016, Rreg. (BE) 2016/679 për Mbrojtjen e Personave Fizik në lidhje me Përpunimin e të Dhënave Personale dhe Lëvizjen e Lirë të këtyre të Dhënave.

18 Shih Komiteti i OKB-së për të Drejtat e Njeriut, *Komenti i Përgjithshëm Nr. 32 mbi Nenin 14: E drejta për barazi para gjykatave dhe për një gjykim të drejtë*, 23 gusht 2007, Dok. i OKB-së CCPR/C/GC/32, paragrafi 2.

penale:¹⁹

- Gëzon të drejtën për një seancë dëgjimore të drejtë dhe publike nga një gjykatë e pavarur dhe e paanshme;
- Duhet të konsiderohet i pafajshëm derisa t'i provohet fajësia sipas ligjit;
- Duhet të kenë kohë dhe lehtësira të mjaftueshme për të përgatitur mbrojtjen e tyre;
- Duhet të jenë në gjendje të mbrohen vetë, ose nëpërmjet një mbrojtësi ligjor që e zgjedhin vetë;
- Duhet të gjykohet brenda një kohe të arsyeshme pa vonesa të panevojshme.

Disa elementë të së drejtës për një gjykim të drejtë mund të kufizohen sipas kushteve të caktuara. Të tjerë elementë – të tillë si supozimi i pafajësisë, e drejta për një seancë dëgjimore nga një gjykatë kompetente, e pavarur dhe e paanshme, si dhe kërkesa që gjykimi në tërësi të jetë i drejtë – konsiderohen absolut dhe nuk mund të kufizohen në asnjë rrethanë.²⁰

E DREJTA PËR LIRINË E SHPREHJES

Liria e shprehjes, siç përcaktohet në Nenin 19 të ICCPR-së dhe Nenin 10 të KEDNJ-së, është një nga bazat e domosdoshme për një shoqëri demokratike. Ajo përfshin të drejtën për të kërkuar, marrë dhe shkëmbyer informacione dhe ide përmes çdo mjeti, pavarësisht kufijve, dhe pa ndërhyrje nga autoriteti publik. Çka është më e rëndësishme, liria e shprehjes zbatohet jo vetëm për informacionin dhe idetë që pranohen si të favorshme, por edhe për ato që mund të fyejnë ose shqetësojnë.²¹ Shtetet pjesëmarrëse të OSBE-së kanë rikonfirmuar se "gjithkush ka të drejtën e lirisë së shprehjes, duke përfshirë të drejtën e komunikimit" dhe "lirinë për të dhënë mendime dhe për të marrë e për të dhënë informacione dhe ide pa ndërhyrje nga autoriteti publik dhe pavarësisht kufijve."²²

Liria e shprehjes mund të jetë objekt i përjashtimeve në rrethana të kufizuara, për shembull për të mbrojtur sigurinë kombëtare ose rendin publik, ose për të parandaluar trazirat ose krimin. Jurisprudenca thekson se këto përjashtime duhet të interpretohen ngushtësisht. Kjo ndihmon për të shmangur ndërhyrjen e tepruar dhe të ashtuquajturin "efekt dekurajues", ku individët vetëcensurohen nga frika se mos u nënshtrohen procedimeve penale (shih kutizën 4).

Interneti ka ofruar mundësi të reja për individët që të ushtrojnë të drejtën e tyre për lirinë e shprehjes duke shkëmbyer informacion gjerësisht dhe me një shpejtësi të jashtëzakonshme. Për shkak të aksesit dhe aftësisë së tij për të ruajtur dhe transmetuar shumë informacione, interneti luan një rol të rëndësishëm në përmirësimin e aksesit publik në lajme dhe lehtësimin e shpërndarjes së informacionit.²³ Megjithatë, këto përfitime shoqërohen nga një sërë rreziqesh,

19 GJEDNJ, *Udhëzues për Nenin 6 të Konventës Evropiane për të Drejtat e Njeriut: E drejta për një gjykim të drejtë (gjykim penal)* (Strasburg, 2022).

20 Shih Komiteti i OKB-së për të Drejtat e Njeriut, *Komenti i Përgjithshëm Nr. 32 mbi Nenin 14: E drejta për barazi para gjykatave dhe për një gjykim të drejtë*, 23 gusht 2007, Dok. i OKB-së CCPR/C/GC/32, paragrafi 6, 19.

21 Departamenti i KE-së për Ekzekutimin e Vendimeve të Gjykatës Evropiane për të Drejtat e Njeriut, *Fleta e të dhënave tematike: Liria e shprehjes*, prill 2021, e disponueshme në <https://rm.coe.int/thematic-factsheet-freedom-expression-eng/1680a235d0>.

22 KSBE/OSBE, *Dokumenti i Kopenhagës 1990*, 27 qershor 1990, CSCE/CHDC.43, paragrafi 9.1.

23 Shih, p.sh., GJEDNJ, *Delfi AS kundër Estonisë [GC]*, 10 tetor 2013, Nr. 64569/09, Neni 133; GJEDNJ, *Times Newspapers Ltd (Nr. 1 dhe 2) kundër Mbretërisë së Bashkuar*, 10 mars 2009, Nr. 3002/03 dhe 23676/03, Neni 27.

ndër të cilat veçanërisht fakti se gjuha e paligjshme, duke përfshirë gjuhën e urrejtjes dhe gjuhën që nxit diskriminimin, armiqësinë ose dhunën, mund të përhapen në mbarë botën brenda pak sekondash, shpesh duke mbetur përgjithmonë në internet.²⁴

Ashtu si në botën jashtë linje, shtetet kanë për detyrë të sigurojnë që çdo kufizim i të shprehurit në internet të jetë **i parashikuar me ligj, i nevojshëm, dhe proporcional**.²⁵

E DREJTA PËR MBROJTJEN E PRONËS

KEDNJ-ja përcakton se njerëzit – dhe shoqëritë – kanë të drejtë të zotërojnë pronën që është ligjërisht e tyre. Kjo përfshin objektet fizike që dikush zotëron, burimet financiare, si depozitat bankare dhe aksionet, si dhe pronësinë intelektuale.²⁶ Prona përfshin, gjithashtu, asete virtuale si kriptomonedhat.

Shtetet nuk mund t'i privojnë individët ose shoqëritë nga prona e tyre, përveç nëse kjo është në interes të publikut dhe i nënshtrohet kushteve të përcaktuara në ligj.

3.3 PARIMET E LIGJSHMËRISË, NEVOJËS DHE PROPORCIONALITETIT

Shumica e të drejtave të njeriut, duke përfshirë të drejtën për privatësi dhe lirinë e shprehjes, nuk janë absolute dhe mund të kufizohen në rrethana të caktuara. Është një parim i konsoliduar i ligjit ndërkombëtar për të drejtat e njeriut që çdo kufizim i tillë i një të drejte duhet të parashikohet me ligj, të jetë i nevojshëm dhe proporcional.

Parimi i **ligjshmërisë** kërkon që çdo masë që kufizon një të drejtë të ketë një bazë në legjisllacionin kombëtar. Kjo bazë ligjore duhet të jetë në dispozicion të atyre që mund të preken dhe mjaftueshëm e qartë për të informuar në mënyrën e duhur individët për rrethanat dhe kushtet në të cilat autoritetet publike gëzojnë të drejtën të marrin masa që prekin të drejtat e tyre. Legjisllacioni duhet të përmbajë masa mbrojtëse të përshtatshme kundër zbatimit arbitrar dhe nuk duhet t'u japë liri të tepërt zyrtarëve, të cilëve u është besuar zbatimi.

Parimi i **nevojës** përbëhet nga dy elemente. Së pari, çdo kufizim i një të drejte duhet **të ndjekë një qëllim të ligjshëm**. Disa të drejta i specifikojnë këto qëllime të ligjshme. Për shembull, KEDNJ-ja lejon që e drejta për respektimin e jetës private dhe familjare dhe e drejta e lirisë së shprehjes të kufizohet në interes të sigurisë kombëtare, sigurisë publike ose për parandalimin e trazirave apo krimit, ndër të tjera. Së dyti, kufizimi duhet të vendoset vetëm në atë masë që është

24 Shih, p.sh., GJEDNJ, *Delfi AS kundër Estonisë [GC]*, 10 tetor 2013, Nr. 64569/09, Neni 110; GJEDNJ, *Annen kundër Gjermanisë*, 20 shtator 2018, Nr. 3682/10, Neni 67.

25 ZKLDNJ (pa datë), *Fleta e të dhënave për Lirinë e Opinionit dhe Shprehjes*, e disponueshme në https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/Factsheet_1.pdf

26 Departamenti i KE-së për Zbatimin e Vendimeve të Gjykatës Evropiane për të Drejtat e Njeriut, *Fleta e të dhënave tematike për mbrojtjen e pronës*, qershor 2022, e disponueshme në <https://rm.coe.int/thematic-factsheet-protection-of-property-eng/1680a6f07f>.

e nevojshme për të arritur këtë qëllim. Me fjalë të tjera, kufizimi nuk duhet të jetë tepër i gjerë ose të zgjasë më shumë se sa është e nevojshme për të arritur qëllimin, d.m.th., ai duhet përcaktuar ngushtësisht dhe të ketë kohëzgjatje të kufizuar.

Parimi i **proporcionalitetit** nënkupton se çdo masë që bie ndesh me një të drejtë duhet të jetë proporcionale me qëllimin e ligjshëm që ndjek. Kjo kërkon që të vërtetohet se nuk ekzistojnë masa më pak kufizuese, se thelbi i së drejtës ruhet dhe se kufizimi i së drejtës nuk është diskriminues. Ekzistenca dhe zbatimi efektiv i masave mbrojtëse procedurale është një aspekt thelbësor për të përcaktuar nëse kufizimi i një të drejte është proporcional.

4

Kompetencat procedurale specifike për krimin kibernetik dhe masat mbrojtëse për të drejtat e njeriut

- 4.1 VEÇORITË E HETIMEVE PËR KRIMIN KIBERNETIK
- 4.2 KOMPETENCAT PROCEDURALE DHE BASHKËPUNIMI
NDËRKOMBËTAR LIDHUR ME KRIMIN KIBERNETIK
- 4.3 MASAT MBROJTËSE SPECIFIKE TË TË DREJTAVE TË NJERIUT
NGA KRIMI KIBERNETIK

4.1 VEÇORITË E HETIMEVE PËR KRIMIN KIBERNETIK

Hetimi dhe ndjekja me sukses e krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale paraqet sfida të veçanta për profesionistët e drejtësisë penale. Së pari, duke qenë se prania fizike ose afërsia me një viktimë nuk është faktor në kryerjen e krimeve kibernetike, autorët mund të jenë në një juridiksion kombëtar të ndryshëm nga viktimat e tyre. Në të vërtetë, mund të ketë shumë autorë, secili i vendosur në një juridiksion të veçantë.

Së dyti, kriminelët po fshehin gjithnjë e më shumë identitetin e tyre duke përdorur shërbime si Tor ose Rrjetet Private Virtuale (VPN), të cilët u mundësojnë atyre të përdorin burimet e internetit me anonimitet relativ. Ata përdorin edhe mjete të ndryshme kodimi për të siguruar të dhënat dhe komunikimin e tyre dhe për të fshehur veprimtaritë e tyre kriminale. Operatorët e rrjetit celular përdorin teknologji si Përkthimi i Adresave të Rrjetit, të cilat e bëjnë të vështirë identifikimin e përdoruesve të internetit nga adresat e tyre të Protokollit të Internetit (IP). E gjithë kjo e bën gjithnjë e më sfiduese atribuirimin e veprave kriminale në hapësirën kibernetike.

Përveç kësaj, shumica e provave për krimet kibernetike – dhe, në fakt, provat thelbësore të shumë krimeve jashtë linje – janë në formën e të dhënave digjitale, të cilat janë në vetvete të paqëndrueshme dhe mund të lëvizin, ndryshohen ose fshihen lehtësisht. Për më tepër, të dhënat shpesh ruhen në "cloud" në serverë që mund të ndodhen në një ose më shumë juridiksione të huaja. Shumë ofrues privatë të shërbimeve mund të kenë akses ose kontroll mbi gjurmët digjitale dhe provat digjitale që lidhen me krimin që po hetohet.

Kjo nënkupton se hetimi i krimeve kibernetike shpesh kërkon bashkëpunim të fortë ndërkombëtar – si me aktorë të drejtësisë penale nga vende të tjera, ashtu edhe me subjekte private si ofruesit shumëkombësh të shërbimeve. Disa lloje të krimit kibernetik, për shembull softuer me viruse të ndryshme ose email biznesi i kompromentuar, kërkojnë kombinim të hetimeve financiare me ato digjitale.

4.2 KOMPETENCAT PROCEDURALE DHE BASHKËPUNIMI NDËRKOMBËTAR LIDHUR ME KRIMIN KIBERNETIK

Veçoritë që lidhen me hetimin e krimeve kibernetike ose krimeve të tjera që përfshijnë prova digjitale nxisin një sërë pyetjesh si:

- Kush ka përdorur/po përdor një adresë IP të caktuar (statike ose dinamike) në një kohë të caktuar?
- Kush ka përdorur/po përdor një adresë email-i ose pseudonim të caktuar në një blog apo rrjet social?
- Cilat janë kushtet për ruajtjen e të dhënave të trafikut, duke përfshirë adresat dinamike IP, nga ofruesit e shërbimeve dhe në cilat kushte mund t'i marrin këto të dhëna aktorët e drejtësisë penale?
- Si të merrni të dhëna për një llogari përdoruesi dhe/ose të dhëna të përmbajtjes nga një ofrues

shumëkombësh shërbimi me bazë jashtë vendit?

- Si të aksesoni, sekuestroni dhe hetoni përmbajtjen e komunikimit elektronik (p.sh., aplikacionet e postës elektronike ose mesazheve) ose të dhënat nga pajisje të ndryshme elektronike, përfshirë ato që janë të koduara?
- Si të monitoroni komunikimin e koduar (në internet)?
- Si të zbuloni dhe gjurmoni pasurinë në internet, transfertat elektronike të parave dhe transaksionet e kriptomonedhave?
- Si të sekuestroni kriptomonedhat ose asetet e tjera virtuale?

Ndërsa hetimi i krimit kibernetik ndjek të njëjtat rregulla procedurale si çdo hetim tjetër penal, siç përcaktohet në legjislacionin përkatës kombëtar, marrja e përgjigjeve për këto pyetje mund të kërkojë gjithashtu që hetuesit të kenë kompetenca të veçanta procedurale.

Konventa e KE-së e vitit 2001 për krimin kibernetik, e njohur gjithashtu si Konventa e Budapestit, është traktati i parë ndërkombëtar për krimet e kryera nëpërmjet internetit dhe rrjeteve të tjera kompjuterike.²⁷ Ajo është e hapur për ratifikimin/aderimin nga shtetet që nuk janë anëtare të KE-së dhe është ratifikuar nga një numër i madh shtetesh nëpër rajone të ndryshme, duke përfshirë shumicën e shteteve pjesëmarrëse të OSBE-së. Konventa siguron kompetenca specifike lidhur me mbledhjen dhe përdorimin e provave digjitale, si dhe për bashkëpunimin ndërkombëtar në kontekstin e hetimeve të krimit kibernetik. Këto kompetenca vlejné si për krimet e varura nga kibernetika, ashtu edhe krimet e mundësuar nga kibernetika, dhe për çdo krim tjetër që përfshin prova digjitale.

Konventa kërkon që Shtetet Palë të integrojnë në legjislacionin e tyre të brendshëm një sërë kompetencash hetimore për qëllime të hetimeve ose procedimeve penale. Këto janë:

- Ruajtja e përshpejtuar e të dhënave kompjuterike të depozituara (Neni 16);
- Ruajtja e përshpejtuar dhe zbulimi i pjesshëm i të dhënave të trafikut (Neni 17);
- Urdhri i prodhimit (Neni 18);
- Kërkimi dhe sekuestrimi i të dhënave kompjuterike të ruajtura (Neni 19);
- Mbledhja në kohë reale e të dhënave të trafikut (Neni 20);
- Përgjimi i të dhënave për përmbajtjen (Neni 21).

Konventa përmban, gjithashtu, dispozita që përbëjnë bazën për bashkëpunimin ndërkombëtar në luftën kundër krimit kibernetik. Këtu përfshihet:

- Informacioni spontan (Neni 26);
- Ruajtja e përshpejtuar e të dhënave kompjuterike të depozituara (Neni 29);
- Zbulimi i përshpejtuar i të dhënave të ruajtura të trafikut (Neni 30);
- Ndihma e ndërsjellë lidhur me qasjen në të dhënat e ruajtura kompjuterike (Neni 31);
- Ndihma e ndërsjellë në mbledhjen në kohë reale të të dhënave të trafikut (Neni 33);
- Ndihma e ndërsjellë lidhur me përgjimin e të dhënave për përmbajtjen (Neni 34).

27 Konventa për Krimin Kibernetik, 23 nëntor 2001, CETS Nr. 185, hyrë në fuqi më 1 korrik 2004.

Veç kësaj, Protokollin e Dytë Shtesë të Konventës së Budapestit u hap për nënshkrim nga Palët në Konventën kryesore në maj 2022. Ai prezanton procedura të reja për rritjen e bashkëpunimit të drejtpërdrejtë me ofruesit dhe subjektet në palët e tjera kontraktore, dhe për përmirësimin e bashkëpunimit ndërkombëtar ndërmjet autoriteteve për zbulimin e të dhënave kompjuterike të ruajtura, duke përfshirë dhe ndihmën e ndërsjellë emergjente.²⁸

Këto kompetenca u ofrojnë profesionistëve të drejtësisë penale mjete të rëndësishme për të zbuluar, hetuar dhe ndjekur me sukses veprat penale të kryera kundër kompjuterëve, ose duke përdorur ata. Megjithatë, zbatimi i tyre mund të ndërhyjë në të drejtat e njeriut dhe liritë themelore. Hetuesit që përdorin këto kompetenca kanë përgjegjësinë të sigurohen që çdo kufizim i të drejtave të njeriut të jetë i bazuar në ligj, i nevojshëm dhe proporcional.

4.3 MASAT MBROJTËSE SPECIFIKE TË TË DREJTAVE TË NJERIUT NGA KRIMI KIBERNETIK

Ndërsa dispozitat e standardeve ndërkombëtare dhe rajonale të të drejtave të njeriut zbatohen për të gjitha hetimet penale, Konventa e KE-së për krimin kibernetik kërkon t'i zbatojë ato në mënyrë specifike për hetimet e krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale. Neni 15 i Konventës kërkon që secila Palë të parashikojë në legjislacionin e saj të brendshëm disa kushte dhe masa mbrojtëse që duhet të zbatohen gjatë përdorimit të kompetencave procedurale të Konventës (shih kutizën 2).

Neni 15 nuk i specifikon këto masa mbrojtëse në detaje, por në vend të kësaj i referohet detyrimeve të shteteve sipas KEDNJ-së dhe ICCPR-së si burimi i masave mbrojtëse. Kjo bën të mundur që dispozita të mbajë parasysh dallimet e rëndësishme që ekzistojnë në tradita të ndryshme ligjore lidhur me mënyrën e zbatimit të masave mbrojtëse.

KUTIZA 2 KONVENTA PËR KRIMIN KIBERNETIK NENI 15 – KUSHTET DHE MASAT MBROJTËSE

1. Secila Palë do të marrë masa që krijimi, zbatimi dhe aplikimi i kompetencave dhe procedurave të parashikuara në këtë seksion t'i nënshtrohen **kushteve dhe masave mbrojtëse** të parashikuara nga legjislacioni i saj i brendshëm, i cili siguron mbrojtjen e duhur të të drejtave dhe lirive të njeriut, duke përfshirë të drejtat që lindin në përputhje me detyrimet që ka marrë përsipër në bazë të Konventës së Këshillit të Evropës të vitit 1950 për Mbrojtjen e të Drejtave dhe Lirive Themelore të Njeriut, Konventës Ndërkombëtare të Kombeve të Bashkuara për të Drejtat Civile dhe Politike të vitit 1966 dhe instrumenteve të tjera ndërkombëtare që zbatohen për të drejtat e njeriut, dhe i cili **do të përfshijë parimin e proporcionalitetit**.
2. Këto kushte dhe masa mbrojtëse, sipas rastit, duke pasur parasysh natyrën e procedurës ose kompetencës në fjalë, ndër të tjera, **përfshijnë mbikëqyrjen gjyqësore ose ndonjë**

28 Protokollin e dytë shtesë të Konventës për krimin kibernetik për bashkëpunimin e zgjeruar dhe zbulimin e provave digjitale, 17 nëntor 2021, CETS Nr. 224.

mbikëqyrje tjetër të pavarur, arsyet që justifikojnë zbatimin dhe kufizimin e fushëveprimit dhe kohëzgjatjes së kësaj kompetence ose procedure.

3. Për aq sa është në përputhje me interesin publik, veçanërisht me administrimin e shëndoshë të drejtësisë, secila Palë merr parasysh ndikimin e kompetencave dhe procedurave në këtë seksion **tek të drejtat, përgjegjësitë dhe interesat e ligjshme të palëve të treta.**

Neni 15 thekson kushtet dhe masat mbrojtëse në vijim:

- Parimi i proporcionalitetit;
- Ekzistenca e mbikëqyrjes gjyqësore, ose një mbikëqyrjeje tjetër të pavarur;
- Nevoja për të specifikuar arsye të qarta që justifikojnë një masë;
- Kufizimi i fushëveprimit dhe kohëzgjatjes së kompetencës ose procedurës – sipas rastit, duke pasur parasysh kompetencën dhe çështjen në fjalë;
- Nevoja për të marrë parasysh ndikimin e kompetencës mbi të drejtat, përgjegjësitë dhe interesat e ligjshme të palëve të treta.

Në terma praktikë, kjo do të thotë që oficerët që hetojnë krimet e dyshuara kibernetike duhet të jenë të vetëdijshëm për ndikimin që veprimet e tyre kanë në të drejtat e përcaktuara në traktatet ndërkombëtare për të drejtat e njeriut.

Parimi i proporcionalitetit përfshin ekuilibrimin e masave hetimore të ndryshme dhe të ngjashme lidhur me hetimin e një krimi kibernetik të caktuar. Kjo nënkupton se ndërhyrjet në të drejtat e njeriut duhet të minimizohen dhe se hetuesit duhet të përdorin mjetet me pasojat më të vogla për të arritur qëllimin e tyre.

Ky ekuilibër është i mundur vetëm nëse ekzistojnë opsione të ndryshme – me më pak ose me më shumë pasoja - në legjislacionin kombëtar. Për shembull, ka dy metoda të mundshme për të siguruar akses në të dhënat e ruajtura nga një ofrues shërbimi. Njëra është përdorimi i një urdhri për ruajtjen dhe prodhimin; tjetra është përdorimi i kontrollit dhe sekuestrimit për të marrë të dhënat. Përgjithësisht, mekanizmi i ruajtjes dhe urdhrit të prodhimit krijon më pak pasoja sesa kontrolli dhe sekuestrimi, i cili kërkon akses në një sasi më të madhe të dhënash dhe kryhet zakonisht në vend. Hetuesit duhet të arsyetojnë qartë se pse ata përdorin një metodë hetimore me më shumë pasoja kur ekzistojnë metoda që krijojnë më pak pasoja.

Në çdo rast, hetuesit duhet të sigurojnë prova të mjaftueshme që një gjykatë ose një organ i pavarur të jetë në gjendje të autorizojë përdorimin e masave hetimore ndërhyrëse. Autoritetet gjyqësore ose autoritete të tjera të pavarura duhet të japin leje për përdorimin e këtyre kompetencave pas një vlerësimi të plotë rast pas rasti. Në varësi të rëndësisë së veprës penale, mund të kërkojnë kushte të posaçme sipas legjislacionit kombëtar. Gjithashtu, profesionistët e drejtësisë penale duhet të garantojnë që kompetencat hetimore ndërhyrëse të mos përdoren më gjatë se sa është rigorozisht e nevojshme për hetimin efektiv të çështjes.

Veç kësaj, Protokollin i Dytë Shtesë i Konventës së Budapestit²⁹ detajon Nenin 14 për mbrojtjen

e të dhënave personale. Kjo dispozitë zbatohet për kompetencat e reja procedurale të parashikuara nga Protokollin i Dytë Shtesë dhe përcakton detyrimet që kanë Palët për të siguruar që aspekte të rëndësishme të të drejtave për privatësi dhe mbrojtjes së të dhënave – siç janë qëllimi dhe përdorimi, cilësia dhe integriteti i të dhënave, të dhënat sensitive, mbajtja e të dhënave, vendimmarrja e automatizuar, siguria e të dhënave dhe shkëmbimi në vijim i të dhënave – të respektohen gjatë zbatimit të këtyre kompetencave.

5

Zbatimi i masave mbrojtëse për të drejtat e njeriut në hetimet e krimit kibernetik



- 5.1 E DREJTA PËR PRIVATËSI
- 5.2 E DREJTA PËR NJË GJYKIM TË DREJTË
- 5.3 E DREJTA PËR LIRINË E SHPREHJES
- 5.4 E DREJTA PËR MBROJTJEN E PRONËS

Ky kapitull zbulon elementet që profesionistët e drejtësisë penale duhet të marrin parasysh për të siguruar që të drejtat e njeriut mbrohen gjatë hetimeve të krimit kibernetik. Ai mbështetet gjerësisht në udhëzimet e dhëna nga jurisprudenca e GJEDNJ-së dhe GJDBE-së. Ky udhëzim është i rëndësishëm edhe për shtetet që nuk janë anëtare të KE-së ose BE-së, pasi ofron shembuj konkretë se si mund të sigurohet respektimi i të drejtave të njeriut në hetimet e krimit kibernetik. Disa vendime veçanërisht të rëndësishme të GJEDNJ-së paraqiten më në detaje në Shtojcën 2.

5.1 E DREJTA PËR PRIVATËSI

Hetimi i krimeve kibernetike dhe krimeve të tjera që përfshijnë prova digjitale mund të ndërhyjnë në të drejtën e privatësisë kur ato:

- Përdorin të dhënat personale;
- Përfshijnë mbajtjen dhe përpunimin e të dhënave të abonentëve, trafikut ose përmbajtjes;
- Ndërhyjnë në privatësinë e komunikimeve, për shembull kur përgjojnë mesazhe ose të dhëna trafiku;
- Përfshijnë mbikëqyrjen sekrete, si operacione të fshehta për kapjen e kriminelëve në tregjet në internet (rrjeti i errët).

Ekziston një organ gjithëpërfshirës i praktikës gjyqësore si nga GJEDNJ-ja ashtu edhe nga GJDBE-ja lidhur me zbatimin e të drejtës së privatësisë.

SHTRIRJA DHE ZBATIMI I TË DREJTËS PËR PRIVATËSI NË HETIMET E KRIMIT KIBERNETIK

Jurisprudenca e GJEDNJ-së ofron udhëzime të detajuara për shtrirjen dhe zbatimin e së drejtës për privatësi në kontekstin e hetimeve të krimit kibernetik. Në praktikën e saj gjyqësore, Gjykata e përcakton gjerësisht shtrirjen e së drejtës për jetën private dhe familjare, në mënyrë që ajo të shtrihet tek:

- Mbrojtja e reputacionit individual, shpifja (detyrim pozitiv i shtetit lidhur me detyrimin e ofruesit të shërbimit);
- Mbrojtja e të dhënave;
- Mbledhja e dosjeve ose e të dhënave nga shërbimet e sigurisë ose organet e tjera të shtetit;
- Mbikëqyrja policore (përfshirë internetin dhe rrjetin e errët³⁰);
- Ndalimi dhe kontrollimi i kompetencave policore;
- Vizita në shtëpi, kërkime dhe sekuestrime;
- Përgjimi i telekomunikacionit në një kontekst hetimi penal;

- Korrespondenca e individëve privatë, profesionistëve dhe shoqërive;
- Mbikëqyrja e fshehtë e qytetarëve dhe organizatave;
- Ruajtja e të dhënave të abonentëve dhe trafikut.³¹

Gjykata ka theksuar gjithashtu se e drejta për jetën private dhe familjare vendos mbi shtetet një detyrim pozitiv (për të mbrojtur të drejtën) dhe një detyrim negativ (të përmbahen nga ndërhyrja në të drejtën). Për shembull, në K.U. kundër Finlandës, Gjykata theksoi detyrimin pozitiv të një shteti për të hetuar krimet në mënyrë efektive dhe për të miratuar legjislacionin e duhur mbi përjashtimet nga detyrimi i ofruesve të shërbimeve për të mbajtur të dhënat konfidenciale.³² Gjykata theksoi se ndërsa liria e shprehjes dhe konfidencialiteti i komunikimit janë konsideratat kryesore, ato nuk mund të jenë absolute. Duke pasur parasysh natyrën serioze të çështjes, Gjykata vendosi se shteti duhet të kishte krijuar një kuadër ligjor për harmonizimin e konfidencialitetit të shërbimeve të internetit me parandalimin e trazirave ose krimit dhe mbrojtjen e të drejtave dhe lirive të të tjerëve.³³

Ashtu si me çdo ndërhyrje në të drejtat e njeriut, kufizimet në të drejtën e privatësisë duhet të parashikohen me ligj, të domosdoshëm dhe proporcional. Jurisprudenca e GJEDNJ-së jep udhëzime se çfarë do të thotë kjo në praktikë. Parime të ngjashme zbatohen për dispozitën përkatëse në ICCPR (Neni 17).³⁴

Për sa i përket **bazave ligjore**, llogjislacioni që autorizon përdorimin e pushteteve që ndërhyjnë në të drejtën e jetës private duhet të jetë i aksesueshëm për ata që mund të preken dhe të ketë qartësi të mjaftueshme në mënyrë që t'u japë "individëve një të dhënë adekuate për rrethanat dhe kushtet në të cilat autoritetet kanë të drejtë të përdorin masa që prekin të drejtat e tyre sipas Konventës."³⁵ Kjo do të thotë se kompetencat e ndryshme procedurale në dispozicion të hetuesve (p.sh., dispozitat për kërkesat për ruajtjen ose prodhimin e të dhënave, për të lejuar mbledhjen në kohë reale të të dhënave të trafikut, ose për të kontrolluar dhe sekuestruar të dhëna kompjuterike, objekte ose dokumente) duhet të përcaktohen qartë në legjislacionin kombëtar.

Për sa i përket **nevojës dhe proporcionalitetit**, çdo ndërhyrje duhet të jetë në ndjekje të një qëllimi të ligjshëm – në këtë rast, hetimi i një krimi të caktuar – dhe i kufizuar në atë që është e nevojshme për të arritur këtë qëllim. Kjo kërkon shqyrtimin nëse ekzistojnë masa alternative më pak kufizuese. Për më tepër, legjislacioni duhet të përmbajë masa mbrojtëse të përshtatshme kundër zbatimit arbitrar dhe të mos u japë liri të tepruar zyrtarëve të cilëve u është besuar zbatimi i tij.

Kjo nënkupton se legjislacioni që përcakton kompetencat procedurale për përdorim në hetimet e krimit kibernetik duhet:

- Të kërkojë ekzistimin e masave mbrojtëse të përshtatshme për justifikimin e përdorimit të kompetencave procedurale individuale;

31 GJEDNJ, *Udhëzues për Nenin 8 të Konventës Evropiane për të Drejtat e Njeriut: E drejta për respektimin e jetës private dhe familjare, shtëpisë dhe korrespondencës* (Strasburg, 2020); Shih gjithashtu: GJEDNJ (2023), *Fleta e të dhënave mbi Mbrojtjen e të Dhënave Personale*, e disponueshme në https://www.echr.coe.int/Documents/FS_Data_ENG.pdf; GJEDNJ (2022), *Fleta e të dhënave mbi Mbikëqyrjen Masive*, e disponueshme në https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.

32 GJEDNJ, *K.U. kundër Finlandës*, 2 dhjetor 2008, Nr. 2872/02, Neni 49.

33 Ibid., Nenet 48, 49.

34 Shih Komiteti i OKB-së për të Drejtat e Njeriut, *CCPR Komenti i Përgjithshëm nr. 16: Neni 17, E drejta për privatësi*, 23 mars 1988, paragrafët 4, 5.

35 GJEDNJ, *Fernández Martínez kundër Spanjës [GC]*, 12 qershor 2014, Nr. 56030/07, Neni 117.

- Të përcaktojë që masa i nënshtrohet një mbikëqyrjeje gjyqësore ose një mbikëqyrje tjetër të pavarur, sidomos kur ajo përfshin akte veçanërisht invazive si përgjimi i të dhënave të përmbajtjes;
- Të përcaktojë afate kohore për ruajtjen e të dhënave;
- Të përjashtojë (ose mbrojë posaçërisht) të dhënat e privileguara nga fushëveprimi i urdhrave të prodhimit dhe kontrollit dhe sekuestrimit.

Shembuj të zbatimit të parimit të proporcionalitetit mund të gjenden në rastet e GJEDNJ-së që lidhen me përgjimin e të dhënave të përmbajtjes, që është kompetenca procedurale më ndërhyrëse e përcaktuar në Konventën e KE-së për Krimin Kibernetik. GJEDNJ-ja është shprehur se, në veçanti, dispozitat ligjore që rregullojnë përgjimin e komunikimeve duhet të sigurojnë garanci të përshtatshme dhe efektive kundër arbitraritetit dhe rrezikut të abuzimit të natyrshëm në çdo sistem të mbikëqyrjes sekrete, dhe ka përcaktuar kushte specifike dhe masa mbrojtëse për mbikëqyrjen e fshehtë të komunikimeve (shih seksionin për “Mbikëqyrjen e fshehtë në hetimet e krimit kibernetik” më poshtë).³⁶

MBROJTJA E TË DHËNAVE PERSONALE NË HETIMET E KRIMIT KIBERNETIK

Një tjetër aspekt i rëndësishëm i së drejtës për privatësi ka të bëjë me të drejtën për mbrojtjen e të dhënave personale, e cila përcaktohet në një sërë instrumentesh ligjore ndërkombëtare dhe rajonale (shih kutizën 3). Parimet e mbrojtjes së të dhënave duhet të merren parasysh gjatë rregullimit të kompetencave policore dhe gjatë mbledhjes dhe përpunimit të të dhënave personale në kontekstin e hetimeve penale. Këto parime përfshijnë:³⁷

- **Ligjshmërinë:** të dhënat personale duhet të përpunohen në mënyrë të ligjshme, ose me pëlqimin e subjektit të të dhënave ose mbi bazën e një arsyeje tjetër legjitime të parashikuar në legjislacionin për mbrojtjen e të dhënave.
- **Drejtësinë:** të dhënat personale duhet të përpunohen në mënyrë të drejtë dhe subjektet e të dhënave duhet të informohen për rrezikun.
- **Transparencën:** të dhënat personale duhet të përpunohen në mënyrë transparente. Subjektet e të dhënave duhet të informohen se si po përdoren të dhënat e tyre.
- **Kufizimin e qëllimit:** çdo përpunim i të dhënave personale duhet të bëhet për një qëllim specifik, të përcaktuar qartë. Çdo përpunim shtesë duhet të jetë në përputhje me qëllimin origjinal.
- **Minimizimin e të dhënave:** përpunimi i të dhënave duhet të kufizohet në atë që është e nevojshme për të përmbushur një qëllim legjitim.
- **Saktësinë e të dhënave:** kontrollorët e të dhënave duhet të sigurojnë që të dhënat personale të jenë të sakta dhe të përditësuara dhe duhet të ndërmarrin hapa për të fshirë ose korrigjuar të dhënat e pasakta.

³⁶ GJEDNJ, *Roman Zakharov kundër Rusisë [GC]*, 4 dhjetor 2015, Nr. 47143/06; GJEDNJ, *Breyer kundër Gjermanisë*, 30 janar 2020, Nr. 50001/12; krahaso edhe me vendimet e GJDBE-së për ruajtjen e të dhënave.

³⁷ Agjencia e BE-së për të Drejtat Themelore dhe KE, *Udhëzues mbi Ligjin Evropian për Mbrojtjen e të Dhënave* (Luksemburg, 2018).

- **Kufizimin e ruajtjes:** të dhënat personale nuk duhet të mbahen më gjatë se sa është e nevojshme dhe duhet të fshihen ose anonimizohen kur të mos nevojiten më për qëllimet për të cilat janë mbledhur.
- **Sigurinë e të dhënave (integriteti dhe konfidencialiteti):** masat e duhura teknike ose organizative duhet të zbatohen gjatë përpunimit të të dhënave personale për të mbrojtur të dhënat nga aksesimi, përdorimi, modifikimi, zbulimi, humbja, shkatërrimi ose dëmtimi aksidental, i paautorizuar ose i paligjshëm.
- **Llogaridhënien:** kontrollorët dhe përpunuesit e të dhënave duhet të zbatojnë në mënyrë aktive dhe të vazhdueshme masa për të promovuar dhe mbrojtur mbrojtjen e të dhënave dhe duhet të jenë në gjendje të demonstrojnë përputhshmërinë me dispozitat për mbrojtjen e të dhënave.

KUTIZA 3 INSTRUMENTET JURIDIKE NDËRKOMBËTARE DHE RAJONALE PËR MBROJTJEN E TË DHËNAVE PERSONALE

- **Konventa e KE-së për Mbrojtjen e Individëve lidhur me Përpunimin Automatik të të Dhënave Personale** e datës 28 janar 1981, nr. 108 (ka hyrë në fuqi në 1985).
- **Protokolli për ndryshimin e Konventës së KE-së për Mbrojtjen e Individëve lidhur me Përpunimin Automatik të të Dhënave Personale**, datë 10 tetor 2018, nr. 223 (nuk ka hyrë ende në fuqi).
- **Rregullorja e Përgjithshme e BE-së për Mbrojtjen e të Dhënave:** Rregullorja (BE) 2016/679 e Parlamentit Evropian dhe e Këshillit e datës 27 prill 2016 për mbrojtjen e personave fizikë lidhur me përpunimin e të dhënave personale dhe për lëvizjen e lirë të këtyre të dhënave, si dhe shfuqizimin e Direktivës 95/46/KE (në fuqi nga 2018).
- **Direktiva e BE-së për zbatimin e ligjit:** Direktiva (BE) 2016/680 e Parlamentit Evropian dhe e Këshillit e datës 27 prill 2016 për mbrojtjen e personave fizikë lidhur me përpunimin e të dhënave personale nga autoritetet kompetente për qëllime të parandalimit, hetimit, zbulimit ose ndjekjes penale të veprave penale ose ekzekutimin e dënimeve penale, dhe mbi lëvizjen e lirë të të dhënave të tilla, dhe shfuqizimin e Vendimit Kuadër të Këshillit 2008/977/JHA (në fuqi nga 2018).

GJEDNJ-ja ka ekzaminuar tashmë një gamë të gjerë ndërhyrjesh në të drejtën e jetës private sipas nenit 8 të KEDNJ si rezultat i ruajtjes, përpunimit dhe përdorimit të të dhënave personale. Këto përfshijnë: përdorimin e mbikëqyrjes përmes GPS-së në hetimet penale;³⁸ zbulimin e informacionit identifikues të autoritetet ligjzbatuese nga ofruesit e telekomunikacionit;³⁹ mbajtja e pacaktuar e gjurmëve të gishtërinjve, mostrave të qelizave dhe profileve të ADN-së pas procedimit penal;⁴⁰ e ashtuquajtura matje ose grumbullimi i të dhënave të përdorimit ose trafikut;⁴¹ dhe ruajtja e të

38 GJEDNJ, *Uzun kundër Gjermanisë*, 2 shtator 2010, Nr. 35623/05; GJEDNJ, *Ben Faiza kundër Francës*, 8 shkurt 2018, Nr. 31446/12.

39 GJEDNJ, *K.U. kundër Finlandës*, 2 dhjetor 2010, Nr. 2872/02; GJEDNJ, *Benedik kundër Sllovenisë*, 24 prill 2018, Nr. 62357/14.

40 GJEDNJ, *S. dhe Marper kundër Mbretërisë së Bashkuar [GC]*, 4 dhjetor 2008, 30562/04 dhe 30566/04.

41 GJEDNJ, *Malone kundër Mbretërisë së Bashkuar*, 2 gusht 1984, Nr. 8691/79; GJEDNJ, *Copland kundër Mbretërisë së Bashkuar*, 3 prill 2007, Nr. 62617/00.

dhënave për përdoruesit e kartave të parapaguara SIM.⁴²

Në çështjen *Marper kundër Mbretërisë së Bashkuar*, GJEDNJ-ja e bëri të qartë se ruajtja e thjeshtë e të dhënave që lidhen me jetën private të një personi përbën ndërhyrje në të drejtën e privatësisë, të sanksionuara në nenin 8 të KEDNJ-së. Gjykata u shpreh se mbrojtja e të dhënave personale është e një rëndësie themelore për gëzimin e së drejtës për respektimin e jetës private dhe familjare. Ligji i brendshëm duhet të sigurojë që të sigurohen masat e duhura mbrojtëse, veçanërisht kur përfshihet përpunimi automatik i të dhënave personale. Në veçanti, ligji vendas duhet të sigurojë që të dhënat e tilla të jenë relevante dhe jo të tepruara lidhur me qëllimet për të cilat ato ruhen, dhe që ato të ruhen në një formë që lejon identifikimin e subjekteve të të dhënave jo më gjatë se sa është e nevojshme për qëllimin për të cilat mbahen ato të dhëna. Ai gjithashtu duhet të ofrojë garanci adekuate që të dhënat personale të ruajtura të mbrohen në mënyrë efektive nga keqpërdorimi.

RUAJTJA DHE AKSESI NË TË DHËNAT E ABONENTIT APO TË TRAFIKUT

Një çështje që lidhet drejtpërdrejt me mbrojtjen e të dhënave personale është mbajtja e të dhënave. Si GJEDNJ-ja ashtu edhe GJDBE-ja e kanë trajtuar këtë çështje në shumë raste. Në *Benedik kundër Sllovenisë*, GJEDNJ-ja gjeti shkelje të nenit 8 të KEDNJ-së në lidhje me mungesën e qartësisë në kuadrin kushtetues Slloven mbi kushtet ligjore për aksesin në të dhënat e abonentit në lidhje me adresat IP (dinamike). Ai zbuloi se përdoruesit e objekteve të aksesit në internet kanë një pritshmëri legjitime për privatësinë, edhe nëse ata me vetëdije zbulojnë adresën e tyre IP për publikun.

Në çështjen *Breyer kundër Gjermanisë*, Gjykata nuk gjeti shkelje të nenit 8 të KEDNJ-së, pasi kushtet dhe masat mbrojtëse të legjisllacionit gjerman që rregullon detyrimin e ofruesve të shërbimeve për të ruajtur të dhënat personale të përdoruesve të kartave SIM të telefonave celularë me parapagesë dhe kushtet sipas të cilave këto të dhëna u vihen në dispozicion autoriteteve sipas kërkesës ishin të qarta dhe proporcionale. Në gjykimin e kësaj çështjeje, Gjykata theksoi rëndësinë themelore të së drejtës për privatësi dhe nevojën për masa mbrojtëse të forta për të parandaluar përdorimin e të dhënave personale në kundërshtim me nenin 8.

Në veçanti, Gjykata konstatoi se mbledhja e emrave dhe adresave të kërkuesve si përdorues të kartave SIM të parapaguara përbente një ndërhyrje të kufizuar në të drejtat e tyre. Ligji në fjalë kishte masa mbrojtëse shtesë dhe njerëzit gjithashtu mund t'u drejtoheshin organeve të pavarura të mbikëqyrjes së të dhënave për të shqyrtuar kërkesat e autoriteteve për të dhëna dhe për të kërkuar korrigjim ligjor nëse është e nevojshme. Prandaj, në këtë rast, Gjermania nuk i kishte tejkaluar kufijtë e gjykimin të saj ("kufiri i vlerësimit") në zbatimin e ligjit në fjalë dhe mbledhja e të dhënave nuk shkel të drejtat e kërkuesve.

Në vitin 2006, BE-ja miratoi të ashtuquajturën Direktivë për Mbajtjen e të Dhënave, e cila rregullonte mbajtjen e disa llojeve të të dhënave të trafikut lidhur me përdorimin e rrjeteve të telekomunikacionit

42 GJEDNJ, *Breyer kundër Gjermanisë*, 30 janar 2020, Nr. 50001/12.

(telefon, celular dhe të dhënat e internetit) për qëllime të drejtësisë penale.⁴³ Të dhënat e trafikut pasqyrojnë përdoruesit aktivitet në rrjet, duke i mundur zbatimin e ligjit, ndër të tjera, të shohin origjinën dhe destinacionin e thirrjeve telefonike në rrjet, të dhënat e vendndodhjes (në rrjetin celular), si dhe adresën IP të përdoruesve të shërbimeve të aksesit në internet. Konkretisht në lidhje me krimin kibernetik, është e rëndësishme të theksohet se kjo Direktivë nuk kërkon mbajtjen e faqeve të internetit të vizituara ose të dhëna të tjera që lidhen me përdorimin e internetit, por kufizohet në mbajtjen e lidhjes midis adresës IP dhe të dhënave të abonentëve të përdoruesve.

Në vitin 2014, GJDBE-ja e shpalli Direktivën e Ruajtjes së të Dhënave të papajtueshme me nenet 7 dhe 8 të Kartës së të Drejtave Themelore të BE-së (respektimi i jetës private dhe familjare dhe mbrojtja e të dhënave personale) dhe për këtë arsye të pavlefshme.⁴⁴ Gjykata vendosi se mbajtja e të dhënave të trafikut të parashikuar nga Direktiva ishte e papajtueshme me të drejtën e privatësisë për shkak të natyrës së saj të përgjithësuar (kërkonte ruajtjen e të dhënave të përdoruesve që nuk dyshohen për ndonjë krimi), mungesën e masave mbrojtëse kundër aksesit dhe përdorimit të paligjshëm të të dhënave, dhe mungesa e kufizimit të qëllimit (përdorimi do të ishte për krime të rënda, por këtij termi i mungonte një përkufizim i qartë në Direktivë).

GJDBE-ja sqaroi më tej pozicionin e saj në disa çështje pasuese lidhur me legjislacionin kombëtar në shtetet anëtare të BE-së që bazohet në Direktivën e Mbajtjes së të Dhënave.⁴⁵ Gjykata konstatoi se këto korniza ligjore kombëtare ishin në kundërshtim me të drejtat për privatësi dhe mbrojtjen e të dhënave, siç kërkohet mbajtjen e përgjithshme dhe pa dallim të të dhënave të trafikut dhe vendndodhjes. Sqaroi se mbajtja e tillë e të dhënave është e lejueshme vetëm nëse është i pranishëm ose i parashikueshëm një kërcënim serioz për sigurinë kombëtare, dhe nëse mbajtja e të dhënave i nënshtrohet një shqyrtimi gjyqësor ose një shqyrtimi tjetër të pavarur dhe është vetëm për një periudhë të kufizuar kohore. Gjithashtu deklaroi se ligji i BE-së nuk e përjashton legjislacionin kombëtar që parashikon ruajtjen e synuar të të dhënave të trafikut dhe vendndodhjes për qëllime të mbrojtjes së sigurisë kombëtare, luftimit të krimeve të rënda dhe parandalimit të kërcënimeve serioze ndaj sigurisë publike, me kusht që të ekzistojnë disa masa mbrojtëse.⁴⁶

Në të njëjtën kohë, Gjykata sqaroi se ligji i BE-së lejon ruajtjen e përgjithshme dhe pa dallim të të dhënave të abonentëve, d.m.th., të dhënave të adresës IP dhe të dhënave lidhur me identitetin civil të përdoruesve, për të njëjtat qëllime.⁴⁷ Nevoja për të ndjekur penalisht krimin (kibernetik) krimi dhe identifikuar përdoruesit keqdashës në internet u konsiderua se peshonte më shumë se ndërhyrja në të drejtën e privatësisë të shkakuar nga mbajtja e të dhënave të kufizuara në adresat IP burimore të përdoruesve të internetit. Kjo i ka hapur derën masave legjislative që parashikojnë mbajtjen parandaluese të adresave IP me qëllim të luftimit të krimit dhe ruajtjes së sigurisë publike. Pa këto të

43 Direktiva 2006/24/KE e Parlamentit Evropian dhe e Këshillit mbi ruajtjen e të dhënave të krijuara ose të përpunuara në lidhje me ofrimin e shërbimeve të komunikimeve elektronike të disponueshme publikisht ose të rrjeteve të komunikimeve publike dhe që ndryshon Direktivën 2002/58/KE, 13 prill 2006, OJEU L 105/54.

44 GJDBE, *Të drejtat digjitale, Ireland Ltd kundër Ministrisë për Komunikime, Burimeve Detare dhe Natyrore dhe të tjerë dhe Kärntner Landesregierung dhe të tjerë* [GC], 8 prill 2014, C-293/12 dhe C-594/12 të bashkuara.

45 GJDBE, *Të Drejta Digjitale Ireland Ltd kundër Ministrisë për Komunikime, Burimeve Detare dhe Natyrore dhe të tjerë dhe Kärntner Landesregierung dhe të tjerë* [GC], 8 prill 2014, bashkuar C-293/12 dhe C-594/12; GJDBE, *Tele2 Sverige AB kundër Post och telestyrelsen dhe Sekretarit të Shtetit për Departamentin e Brendshëm kundër Tom Watson dhe të tjerë* [GC], 21 dhjetor 2016, bashkuar C-203/15 dhe C-698/15; GJDBE, *Privacy International kundër Sekretarit të Shtetit për Çështjet e Jashtme dhe të Komunuelthit dhe të tjerë* [GC], 6 tetor 2020, C-623/17; GJDBE, *La Quadrature du Net dhe të tjerë kundër Premier ministre dhe të tjerë* [GC], 6 tetor 2020, të bashkuara C-511/18, C-512/18 dhe C-520/18; GJDBE, *SpaceNet dhe Telekom Deutschland GmbH* [GC], 27 tetor 2022, të bashkuara C-793/19 dhe C-794/19.

46 GJDBE, *SpaceNet dhe Telekom Deutschland GmbH* [GC], 27 tetor 2022, bashkuar C-793/19 dhe C-794/19.

47 GJDBE, *La Quadrature du Net dhe të tjerë kundër Kryeministrit dhe të tjerë* [GC], 6 tetor 2020, të bashkuara C-511/18, C-512/18 dhe C-520/18; GJDBE, *SpaceNet dhe Telekom Deutschland GmbH* [GC], 27 tetor 2022, të bashkuara C-793/19 dhe C-794/19.

dhëna, përdorimi i internetit mund të bëhet tërësisht anonim, me pasoja të rëndësishme për hetimin dhe ndjekjen penale të krimit (kibernetik).

MBIKQYRJA E FSHEHTË NË HETIMET E KRIMIT KIBERNETIK

Metodat e ndryshme të hapura dhe të fshehta të mbledhjes së informacionit paraqesin shkallë të ndryshme të ndërhyrjes në të drejtën e privatësisë. Disa nga këto metoda, si përdorimi i teknikave speciale të hetimit dhe masave të tjera të fshehta të hetimit, duke përfshirë mbikëqyrjen në ambiente private ose në shtëpi, përgjimin e komunikimeve, përdorimin e agjentëve dhe informatorëve sekret si dhe aksesin në llogari bankare dhe informacione të tjera konfidenciale, janë hulumtuar më në detaje në manualin e OSBE-së për *Të drejtat e njeriut në hetimet kundër terrorizmit*.⁴⁸

Në krahasim me mbikëqyrjen e synuar, e cila zakonisht bazohet në dyshime të mëparshme dhe i nënshtrohet autorizimit gjyqësor ose ekzekutiv, programet e mbikëqyrjes masive nuk lejojnë një vlerësim individual rast pas rasti të proporcionalitetit përpara se të merren masa të tilla. Si të tilla, ato rrezikojnë të dëmtojnë vetë thelbin e të drejtës së privatësisë. Informacioni i mbledhur për qëllime të inteligjencës ndonjëherë përdoret gjithashtu si provë në procedurat penale. Megjithatë, qëllimi origjinal i mbledhjes së një informacioni të tillë është i ndryshëm nga qëllimi i ndjekjes penale të krimeve kibernetike ose krimeve të tjera që përfshijnë dëshmi elektronike, dhe shpesh rregulla dhe kushte të ndryshme ligjore zbatohen për mbledhjen e tij. Prandaj, kërkohet qartë kujdes kur përdorni informacion në procedurat penale. Përdorimi i inteligjencës së marrë me mjete të paligjshme në procedurat penale do të jetë në kundërshtim me të drejtat e njeriut.

GJEDNJ-ja ka gjetur shkelje të Nenit 8 të KEDNJ-së në disa raste që lidhen me regjimet e mbikëqyrjes sekrete, duke përfshirë përgjimin në masë të komunikimeve dhe shkëmbimin e inteligjencës, për shembull, *Roman Zakharov kundër Ruisë*,⁴⁹ *Szabó dhe Vissy kundër Hungarisë*,⁵⁰ dhe *Big Brother Watch dhe Të tjerët kundër Mbretërisë së Bashkuar*.⁵¹ Vendimi *Vissy kundër Hungarisë* bëri të qartë se mbikëqyrja gjyqësore e përgjimit sekret është e një rëndësie të veçantë. Një organ i pavarur gjyqësor duhet të mbikëqyrë përdorimin e tyre; një organ i lidhur drejtpërdrejt me ekzekutivin (në këtë rast Ministri i Brendshëm) nuk e plotëson këtë kërkesë. Aktgjykimi gjithashtu theksoi çështjen në lidhje me shtrirjen e masave të mbikëqyrjes dhe konsideroi masat mbrojtëse të parashikuara në legjislacion si të pamjaftueshme të sakta, efektive dhe gjithëpërfshirëse për urdhrin, zbatimin dhe korrigjimin e mundshëm të këtyre masave.

Në *Big Brother Watch dhe të tjerët kundër Mbretërisë së Bashkuar*, Gjykata deklaroi se çdo regjim i përgjimit në masë duhet t'i nënshtrohet “masave mbrojtëse njëra pas tjetrës” në nivelin brenda vendit, që nënkupton: një vlerësim i nevojës dhe proporcionalitetit të masave të marra duhet të bëhet në çdo fazë të procesit; përgjimi në masë duhet t'i nënshtrohet autorizimit të pavarur që në fillim, kur përcaktohen objekti dhe qëllimi i operacionit; dhe se operacioni duhet t'i nënshtrohet

48 Shih gjithashtu OSBE/ODIHR, *Të drejtat e njeriut në hetimet kundër terrorizmit: Një Manual Praktik për Oficerët e Zbatimit të Ligjit* (Varshavë, 2013).

49 GJEDNJ, *Roman Zakharov kundër Ruisë* [GC], 4 dhjetor 2015, Nr. 47143/06.

50 GJEDNJ, *Szabó dhe Vissy kundër Hungarisë*, 12 janar 2016, Nr. 37138/14.

51 GJEDNJ, *Big Brother Watch dhe të tjerët kundër Shteteve të Bashkuara* [GC], 25 maj 2021, Nr. 58170/13, 62322/14 dhe 24960/15.

mbikëqyrjes dhe rishikimit të pavarur të mëvonshëm.⁵²

Në çështjen e lidhur të *Centrum För Rättvisa kundër Suedisë*, Gjykata theksoi mangësitë në kuadrin ligjor vendas që nuk u kompensuan mjaftueshëm nga masa të tjera mbrojtëse.⁵³ Këto përfshinin: mungesën e një rregulli të qartë për shkatërrimin e materialit të përgjuar që nuk përmban të dhëna personale; mungesa e detyrimit për të marrë parasysh privatësinë e individëve kur vendoset nëse do t'u transmetohet materiali i inteligjencës partnerëve të huaj; dhe mungesa e një rishikimi efektiv të mëvonshëm, siç është mundësia që anëtarët e publikut të marrin vendime të arsyetuara në përgjigje të pyetjeve lidhur me përgjimin në masë të komunikimeve.

Këto raste ofrojnë udhëzime të qarta për disa nga masat mbrojtëse të kërkuara në kontekstin e mbikëqyrjes sekrete të komunikimeve. GJEDNJ-ja ka treguar se pret që të ketë një regjim mbikëqyrjeje të pavarur për përdorimin e këtyre kompetencave të fshehta dhe ndërhyrëse dhe se sa më i pavarur të jetë një organ autorizues ose rishikues, aq më shumë ka gjasa që regjimi autorizues dhe rishikues të jetë i përshtatshëm. Në të vërtetë, në *Klass kundër Gjermanisë*, GJEDNJ-ja vuri në dukje se kontrolli gjyqësor i procedurës së autorizimit ofron “garancitë më të mira të një procedure të pavarur, të paanshme dhe të duhur.”⁵⁴ Përdorimi i komisionerëve dhe gjykatave të specializuara në nivel kombëtar mund të plotësojë gjithashtu kërkesat e KEDNJ-së Neni 8.

5.2 E DREJTA PËR NJË GJYKIM TË DREJTË

Hetimet e krimit kibernetik përfshijnë një sërë procesesh që lidhen me elementët kryesorë të së drejtës për një gjykim të drejtë, duke përfshirë:

- Aksesit në të dhënat e ruajtura në pajisje elektronike;
- Mirëmbajtja e integritetit të provave elektronike të sekuestruara në kuadër të kërkimit, sekuestrimit dhe menaxhimit të të dhënave elektronike;
- Aksesit në prova dhe inspektimin e tyre nga i akuzuari lidhur me provat digjitale të sekuestruara;
- Përrjashtimi ose kufizimet e vendosura në kërkimet e komunikimeve dhe informacioneve të privilegjuara (siç janë komunikimet me avokatët, të dhënat mjekësore ose komunikimet e gazetarëve me burimet e tyre).

Prezumimi i pafajësisë është i lidhur ngushtë me të drejtën për të mos fajësuar veten dhe për të heshtur.⁵⁵ E drejta për të heshtur është veçanërisht e rëndësishme në kontekstin e kërkimit dhe hetimit të të dhënave elektronike. Ndërsa legjislacioni kombëtar mund të vendosë sanksione (administrative) ndaj një dëshmitari që nuk është i gatshëm të japë informacion, si për shembull një fjalëkalim për të hyrë në një kompjuter gjatë një kontrolli të pajisjeve elektronike, sanksionimi i një të dyshuari do të ishte problematik, pasi i dyshuari mund të kërkojë të drejtën e tij/saj për të

52 Ibid.

53 GJEDNJ, *Centrum För Rättvisa kundër Suedisë* [GC], 25 maj 2021, Nr. 35252/08.

54 GJEDNJ, *Klass dhe të tjerë kundër Gjermanisë*, 6 shtator 1978, Nr. 5029/71.

55 GJEDNJ, *Udhëzues për Nenin 6 të Konventës Evropiane për të Drejtat e Njeriut: E drejta për një gjykim të drejtë (gjykim penal)* (Strasburg, 2022), paragrafi 197 dhe 373.

heshtur. Prandaj është e rëndësishme që një i dyshuar të vihet në dijeni për të drejtat e tij ose të saj përpara se t'i kërkohet të japë në mënyrë vullnetare një fjalëkalim ose kod aksesi në një kompjuter ose pajisje tjetër elektronike.⁵⁶

Një pajisje ruajtëse, si një disk kompjuteri i brendshëm ose i jashtëm, një disk USB ose një pajisje celulare, mund të përmbajë një sasi të madhe të dhënash që nuk mund të kërkohen gjatë një kontrolli shtëpie. Prandaj, shpesh duhet të sekuestrohet dhe të kontrollohet në një fazë të mëvonshme.⁵⁷ Legjislacioni vendas, duke përfshirë rregullat specifike për kërkimin dhe sekuestrimin (ose më saktë: aksesin dhe kopjimin⁵⁸) të provave digjitale, duhet të garantojë që të ruhet e drejta për një mbrojtje efektive në të njëjtën mënyrë si për provat e prekshme. Dispozitat përkatëse procedurale përfshijnë: detyrimin për të sekuestruar një pajisje elektronike dhe për të krijuar një kopje të saktë; detyrimin për të informuar dhe ftuar të dyshuarin dhe avokatin e tij/saj në kontrollin e pajisjes elektronike të sekuestruar; dhe detyrimin për të zbuluar provat e sekuestruara për mbrojtjen. Vendosja e këtyre masave mbrojtëse procedurale ndihmon për të siguruar që parimet e barazisë së armëve dhe një procedurë kundërshtuese, të cilat janë komponentë të rëndësishëm të një gjykimi të drejtë, të zbatohen në praktikë.

Vëllimi i madh i të dhënave të përfshira në disa hetime paraqet gjithashtu një sfidë për sa i përket zbulimit të të dhënave. Një mbrojtje e rëndësishme është të sigurohet që mbrojtja të ketë mundësinë të marrë pjesë në përcaktimin e kriterëve të përdorura për të përcaktuar se cilat të dhëna mund të jenë të rëndësishme për zbulimin.⁵⁹ Kjo është veçanërisht e rëndësishme në rastet që përfshijnë të dhëna të ruajtura në internet. Për më tepër, çdo refuzim për të lejuar mbrojtjen të kryejë kontrolle të mëtejshme të të dhënave të rastit të identifikuar ose të etiketuar (p.sh., të dhënat që rezultojnë nga një kërkim) shtron çështjen e ofrimit të lehtësive adekuate për përgatitjen e mbrojtjes.⁶⁰ Kudo që është e mundur, mbrojtja duhet të informohet për kriteret e kërkimit për grupe të mëdha të dhënash, t'i jepet akses i barabartë dhe të ketë çdo mundësi për të kërkuar grupet e të dhënave për të dhëna (shfajësuese) përkatëse. Natyra e privilegjuar e komunikimit ndërmjet avokatëve dhe klientëve të tyre duhet respektuar edhe gjatë kërkimit nëpërmjet provave digjitale.

Me pak fjalë, e drejta për një gjykim të drejtë kërkon një procedurë të drejtë dhe të balancuar, veçanërisht kur kërkohen provat digjitale lidhur me kriteret e identifikuar nga autoritetet e drejtësisë penale. Nuk është e pranueshme që të përjashtohet mbrojtja nga ky proces dhe duhet të sigurohen masa mbrojtëse dhe mundësi adekuate për të gjetur prova shfajësuese.

Së fundi, koncepti i një “gjykate të themeluar me ligj”, së bashku me konceptet e “pavarësisë” dhe “paanësisë” së gjykatës, janë pjesë e “kërkesave institucionale” të nenit 6 të KEDNJ-së. Në praktikën gjyqësore të GJEDNJ-së, ekziston një ndërlidhje shumë e ngushtë midis këtyre koncepteve.⁶¹ Ndërsa secili prej tyre shërben për qëllime specifike si garanci të veçanta të gjyqimit të drejtë, ekziston një temë e përbashkët që kalon përmes kërkesave institucionale, në atë që ato udhëhiqen nga qëllimi

56 Konventa mbi krimin kibernetik, 23 nëntor 2001, CETS Nr. 185, Neni 32(b).

57 KE, *Raport Shpjegues për Konventën e Krimit Kibernetik* (Budapest, 2001), Neni 187.

58 Ibid. Nenet 137, 191 dhe 197.

59 GJEDNJ, *Sigurður Einarsson dhe të tjerë kundër Islandës*, 4 qershor 2019, Nr. 39757/15, Neni 90; shih gjithashtu GJEDNJ, *Rook kundër Gjermanisë*, 25 korrik 2019, Nr. 1586/15, Nenet 67, 72.

60 GJEDNJ, *Sigurður Einarsson dhe të tjerë kundër Islandës*, 4 qershor 2019, Nr. 39757/15, Neni 91; shih gjithashtu: KE, *Raporti shpjegues për Konventën e Krimit Kibernetik* (Budapest, 2001), Neni 179.

61 GJEDNJ, *Guðmundur Andri Ástráðsson kundër Islandës* [GC], 1 dhjetor 2020, Nr. 26374/18, Neni 218.

për të mbështetur parimet themelore të shtetit ligjor dhe të ndarjes së pushteteve.⁶²

Në *Szabo dhe Vissy kundër Hungarisë*, GJEDNJ-ja përsëriti lidhjen midis pavarësisë së një organi mbikëqyrës gjyqësor dhe të drejtës për një gjykim të drejtë.⁶³ Po kështu, GJDBE-ja ka identifikuar mbikëqyrjen e mekanizmave të ruajtjes së të dhënave si një mbrojtje të rëndësishme në praktikën e saj gjyqësore.

5.3 E DREJTA PËR LIRINË E SHPREHJES

GJEDNJ-ja ka pranuar në mënyrë të përsëritur se përmbajtja e krijuar nga përdoruesit në internet ofron një platformë të paprecedentë për ushtrimin e lirisë së shprehjes.⁶⁴ TSidoqoftë, Gjykata ka theksuar gjithashtu rreziqet e paraqitura nga përmbajtja ilegale në internet, duke përfshirë pornografinë me fëmijë, gjuhën e urrejtjes dhe gjuhën që nxit dhunë.⁶⁵

E drejta e lirisë së shprehjes mund të ndikohet në mënyrë të drejtpërdrejtë ose të tërthortë nga hetimet e krimit kibernetik:

- Ndërhyrja e drejtpërdrejtë me të drejtën e lirisë së shprehjes ndodh kur bllokohen ose fshihen faqet e internetit dhe e bëjnë përmbajtjen të padisponueshme për shkak të natyrës së saj të paligjshme (p.sh., pornografia me fëmijë, tregjet në internet me mallra dhe shërbime të paligjshme, gjuha e urrejtjes);
- Pengimi indirekt i lirisë së fjalës mund të ndodhë nëse ofruesve të shërbimeve ose përdoruesve të internetit u bëhet presion për të censuruar përmbajtjen me kërcënimin e sanksioneve ose procedurës penale.

Përveç kësaj, hetuesit duhet të balancojnë mbrojtjen e të drejtave të personalitetit (p.sh., shpifjen) dhe nevojën për të ruajtur sigurinë publike, me detyrimin që të garantojnë lirinë e fjalës.

BLLOKIMI I AKSESIT NË INTERNET

Organet ndërkombëtare të të drejtave të njeriut kanë theksuar në mënyrë të përsëritur se bllokimi i mandatuar nga shteti i të gjitha faqeve të internetit, adresave IP, porteve ose protokolleve të rrjetit është një masë ekstreme që është e lejueshme vetëm si masë e fundit dhe nëse respektohen garancitë minimale të procesit të rregullt ligjor.⁶⁶ Masat e bllokimit të faqeve të internetit mund të jenë në përputhje me standardet ndërkombëtare për lirinë e shprehjes vetëm nëse ato parashikohen me ligj dhe janë të nevojshme dhe proporcionale për të mbrojtur qëllimet e

62 Ibid., Nenet 218, 232, 233; shih gjithashtu: KE, *Raporti Shpjegues për Konventën e Krimit Kibernetik* (Budapest, 2001), Neni 70.

63 GJEDNJ, *Szabó dhe Vissy kundër Hungarisë*, 12 janar 2016, Nr. 37138/14.

64 Shih GJEDNJ, *Udhëzues për Nenin 10 të Konventës Evropiane për të Drejtat e Njeriut, Liria e shprehjes* (Strasburg, 2022), Nenet 588–632.

65 GJEDNJ, *Delfi AS kundër Estonisë* [GC], 10 tetor 2013, Nr. 64569/09, Neni 110; GJEDNJ, *Annen kundër Gjermanisë*, 20 shtator 2018, Nr. 3682/10, Neni 67.

66 Shih Përfaqësuesi i OKB-së i OSBE-së për Lirinë e Medias dhe të tjerëve, *Deklarata e Përbashkët për Lirinë e Shprehjes dhe "Lajme të rreme", Dezinformim dhe Propagandë*, 3 mars 2017, FOM.GAL/3/17.

ligjshme.⁶⁷

Në praktikën e saj gjyqësore, GJEDNJ-ja ka theksuar se bllokimi i aksesit në internet mund të jetë në kundërshtim të drejtpërdrejtë me paragrafin 1 të Nenit 10 të KEDNJ-së, që garanton lirinë e shprehjes “pavarësisht kufijve.”⁶⁸ Në çështjen *Bulgakov kundër Ruisë* bëhej fjalë për bllokimin e një faqe interneti të tërë me vendim gjykate për shkak të pranisë së materialit të paligjshëm (edhe pasi ai material ishte hequr). Në vendimin e saj, Gjykata zbuloi se nuk kishte asnjë bazë ligjore për urdhrin e bllokimit, pasi legjislacioni mbi të cilin bazohej urdhri nuk i lejonte autoritetet të bllokoni aksesin në një faqeje të tërë interneti. Gjykata gjithashtu u shpreh se konstatimi i saj i paligjshmërisë zbatohet veçanërisht për bllokimin e vazhdueshëm të faqes së internetit pasi materiali i ndaluar ishte hequr.

Në një çështje të veçantë, *Cengiz dhe të tjerët kundër Turqisë*, në lidhje me bllokimin e faqes së pritjes së videove YouTube, GJEDNJ u shpreh se kërkuesit, të cilët ishin përdorues të faqes, mund të pretendonin në mënyrë të ligjshme se masa kishte prekur të drejtën e tyre për të marrë dhe të japë informacion ose ide. Duke pasur parasysh karakteristikat unike të platformës, aksesit të saj dhe, mbi të gjitha, ndikimin e saj të mundshëm, dhe duke pasur parasysh se nuk kishte alternativa të disponueshme për kërkuesit, Gjykata konstatoi se bllokimi cenonte lirinë e tyre të shprehjes.⁶⁹

PËRGJEGJËSIA PËR PËRMBAJTJEN ONLINE

Ndërkohë që pranon përfitimet e rëndësishme të internetit për ushtrimin e lirisë së shprehjes, GJEDNJ ka shprehur se përgjegjësia për komentet fyese ose lloje të tjera të gjuhës së papërshtatshme duhet, në parim, të mbahet dhe përbën një mjet juridik efektiv për shkeljet e të drejtave të personalitetit.⁷⁰

Në vlerësimin në çështjen *Delfi AS kundër Estonisë* nëse një pronar i një portali lajmesh në internet duhet të heqë komentet e postuara nga një palë e tretë, Gjykata identifikoi katër aspekte të rëndësishme për përcaktimin e përgjegjësisë së ofruesve të shërbimeve për përmbajtjen në platformat e tyre:⁷¹

- Konteksti i komenteve;
- Masat e aplikuara nga shoqëria kërkuese për të parandaluar ose hequr komentet fyese;
- Përgjegjësia e autorëve aktualë të komenteve si një alternativë ndaj përgjegjësisë së shoqërisë kërkuese;
- Pasojat e proceseve të brendshme për shoqërinë kërkuese.

67 Shih, p.sh., OSBE, *Standardet Ndërkombëtare dhe Qasjet Krahasuese mbi Lirinë e Shprehjes dhe Bllokimi i Përmbajtjes Terroriste dhe “Ekstremiste” në internet (Vjenë, 2018)*, paragrafi 47; shih gjithashtu: OSBE/ODIHR, *Komente mbi disa Akte Ligjore që Rregullojnë Komunikimet Masive, Teknologjitë e Informacionit dhe përdorimin e internetit në Uzbekistan* (Varshavë, 2019), paragrafi 86–89.

68 GJEDNJ, *Ahmet Yıldırım kundër Turqisë*, 18 dhjetor 2012, Nr. 3111/10, Neni 67.

69 GJEDNJ, *Cengiz dhe të tjerët kundër Turqisë*, 1 dhjetor 2015, Nr. 48226/10 dhe 14027/11, Nenet 52, 53, 55; shih gjithashtu: GJEDNJ, *Ahmet Yıldırım kundër Turqisë*, 18 dhjetor 2012, Nr. 3111/10, Neni 49, 55 lidhur me një rast të ngjashëm në lidhje me aksesin në një faqe interneti të vendosur në një shërbim pritës të faqeve të Google.

70 GJEDNJ, *Delfi AS kundër Estonisë* [GC], 10 tetor 2013, Nr. 64569/09, Neni 110.

71 GJEDNJ, *Delfi AS kundër Estonisë* [GC], 10 tetor 2013, Nr. 64569/09, Nenet 142–143; shih gjithashtu: GJEDNJ, *Magyar Tartalomszolgáltatók Egyesülete dhe Index.hu Zrt kundër Hungarisë*, 2 shkurt 2016, Nr. 22947/13, Neni 60 e në vazhdim.

Duke zbatuar këto konsiderata, Gjykata vendosi se një sistem njoftimi dhe heqjeje, nëse shoqërohet me procedura efektive që lejojnë reagimin e shpejtë, mund të ofrojë një qasje mjaftueshëm të balancuar për të drejtat e palëve të treta.⁷² Kështu, ofruesit e shërbimeve mund të mbështeten në një sistem të tillë pa tërhequr drejtpërdrejt përgjegjësinë për përmbajtjen e krijuar nga përdoruesit, siç janë komentet fyese.⁷³ Megjithatë, Gjykata nënvizoi gjithashtu se në raste të tilla si *Delfi AS kundër Estonisë*, ku komentet nga përdoruesit e palëve të treta marrin formën e gjuhës së urrejtjes dhe kërcënimeve të drejtpërdrejta kundër integritetit fizik të individëve, të drejtave dhe interesave të tjerëve dhe të shoqërisë si një e tërë mund t'u japë të drejtë Shteteve të vendosin përgjegjësi për portalet e lajmeve në internet nëse nuk marrin masa për të hequr pa u vonuar komentet qartësisht të paligjshme, madje edhe pa njoftim nga viktimat e pretenduar ose palët e treta.

KUTIZA 4 EFEKTI “I FRIKËS” NË LIRINË E SHPREHJES

Për shembull, nëse një faqe interneti me video, përballet me legjislacion të paqartë, ai mund të censurojë jashtë mase përdoruesit në mënyrë që të qëndrojë jashtë telasheve me autoritetet. Ky efekt, i referuar shpesh si një efekt “frike”, mund të parandalohet duke pasur rregulla të qarta, si dhe regjime që kufizojnë përgjegjësinë e ofruesve të shërbimeve në rastet kur ka përmbajtje potencialisht të paligjshme në platformat e tyre pa dijeninë ose lejen e tyre. Një efekt frike në lirinë e shprehjes mund të ndodhë gjithashtu nëse njerëzit vetëcensurojnë veten si rezultat i mbikëqyrjes ose nga frika se mos janë në shënjestër të dyshimeve të gabuara. Kjo, nga ana tjetër, është shpesh rezultat i normave të paqarta ose arbitrare.

BALANCIMI I SË DREJTËS PËR LIRINË E SHPREHJES, PRIVATËSINË DHE PARANDALIMIN E KRIMIT

GJEDNJ-ja ka trajtuar gjithashtu nevojën për të balancuar të drejtat për lirinë e shprehjes dhe privatësinë me përgjegjësinë e shteteve për të parandaluar dhe hetuar krimet. Në *K.U. kundër Finlandës*, Gjykata vendosi se ishte e papajtueshme me nenin 8 të KEDNJ-së të mos detyrohej një ofrues shërbimi të zbulonte identitetin e një personi të kërkuar për vendosjen e një reklame të pahijshme për një të mitur në një faqe takimesh në internet, duke iu referuar në këtë kontekst potencialit kërcënim fizik i të miturit dhe mirëqenien mendore dhe cenueshmërinë e shkaktuar nga mosha e tij/saj e re.⁷⁴ Gjykata deklaroi se megjithëse liria e shprehjes dhe konfidencialiteti i komunikimit janë konsideratat kryesore dhe përdoruesit e internetit duhet të kenë një garanci se privatësia e tyre dhe liria e shprehjes do të respektohet, një garanci e tillë nuk mund të jetë absolute. Ai duhet t'i nënshtrohet me raste imperativave të tjera legjitime, të tilla si parandalimi i çrregullimit ose krimit, ose mbrojtja e të drejtave dhe lirive të të tjerëve.⁷⁵

72 GJEDNJ, *Delfi AS kundër Estonisë* [GC], 10 tetor 2013, Nr. 64569/09, Neni 159.

73 GJEDNJ, *Magyar Tartalomszolgáltatók Egyesülete dhe Index.hu Zrt kundër Hungarisë*, 2 shkurt 2016, Nr. 22947/13, Neni 91; shih gjithashtu: GJEDNJ, *Rolf Anders Daniel Pihl kundër Suedisë*, 7 shkurt 2017, Nr. 74742/14, Neni 32; GJEDNJ, *Tamiz kundër Mbretërisë së Bashkuar*, 19 shtator 2017, Nr. 3877/14, Neni 84; GJEDNJ, *Høiness kundër Norvegjisë*, 19 mars 2019, Nr. 43624/14, Nenet 73–74 lidhur me rëndësinë e reagimit në kohë pas njoftimit për paligjshmërinë e përmbajtjes.

74 GJEDNJ, *K.U. kundër Finlandës*, 2 dhjetor 2008, Nr. 2872/02, Neni 41.

75 *Ibid.*, Neni 49.

Për ta përmbledhur, liria e shprehjes mund të kufizohet vetëm me ligj. Legjislacioni duhet të përcaktojë rregulla dhe kushte të sakta për bllokimin dhe heqjen e faqeve të internetit ose përmbajtjes dhe të kufizojë përgjegjësinë e ofruesve të shërbimeve për përmbajtjen e gjeneruar nga përdoruesit. Kur policia propozon një masë në lidhje me përmbajtjen e paligjshme në internet dhe një gjykatë merr parasysh autorizimin e saj, ndikimi në lirinë e shprehjes duhet të vlerësohet plotësisht për të shmangur ndërhyrjet e tepruara. Duhet të arrihet një ekuilibër, veçanërisht në lidhje me lirinë e medias dhe në rastet e shpifjes ose gjuhës së urrejtjes, ku kufijtë midis përmbajtjes së supozuar të paligjshme dhe shprehjes së një opinioni, pikëpamjet kritike ose politike nuk janë gjithmonë të qarta. Efekti i frikës që censura ka në shoqëri është një aspekt tjetër i rëndësishëm (shih kutinë 4). Bllokimi i faqeve të internetit duhet të kufizohet rreptësisht në përmbajtje kriminale dhe nuk duhet të ndikojë në përmbajtje që nuk është e paligjshme.

5.4 E DREJTA PËR MBROJTJEN E PRONËS

Hetimet e krimit kibernetik shpesh përfshijnë asete virtuale, të cilat mund të sekuestrohen si dëshmi të një krimi dhe/ose të konfiskohen si të ardhura nga krimi. Pronat virtuale më të zakonshme në këtë kontekst janë kriptomonedhat, të cilat shpesh përdoren si një metodë pagese për mallrat e paligjshme të ofruara në tregjet e rrjetit të errët ose për shpërbllim në rastet e softuerit me viruse të ndryshme. Kriptomonedhat kanë një vlerë tregu dhe kështu mund të konsiderohen si “pronë” sipas standardeve ndërkombëtare.

Përdorimi i kriptomonedhave ose aseteve të tjera virtuale nuk është në vetvete i paligjshëm, edhe nëse është i parregulluar në shumë vende. Standardet kundër pastrimit të parave të Task Forcës së Veprimit Financiar (FATF), megjithatë, kërkojnë rregullim të disa aspekteve të kriptomonedhave dhe një numër në rritje vendesh po zbatojnë rregulla për ofruesit e shërbimeve të kriptomonedhave, për shembull në lidhje me krijimin e një portofoli, ruajtjeje, shkëmbimi me monedhën fiat ose me kriptomonedhat të tjera ose asete virtuale.

Heqja dorë nga asetet dhe konfiskimi në përgjithësi konsiderohen nga GJEDNJ-ja si kontroll i përdorimit të pronës, që duhet të konsiderohet sipas Nenit 1 (2) të Protokollit Nr.1 të KEDNJ-së. Gjykata shqyrtoi masat e ndryshme të marra për të luftuar pasurimin e paligjshëm nga të ardhurat nga krimi. Shtetet kanë një kufi të gjerë vlerësimi në zbatimin e politikave për të luftuar krimin, duke përfshirë konfiskimin e:

- Prona që supozohet se ka origjinë të paligjshme;⁷⁶
- Prona të blera me fonde të paligjshme;⁷⁷
- Të ardhurat e veprës penale;⁷⁸

76 GJEDNJ, *Raimondo kundër Italisë*, 22 shkurt 1994, Nr. 12954/87; *Riela dhe të tjerë kundër Italisë*, 4 shtator 2001, Nr. 52439/99; GJEDNJ, *Arcuri dhe të tjerë kundër Italisë*, 5 korrik 2001, nr. 52024/99; GJEDNJ, *Gogitidze dhe të tjerë kundër Gjeorgjisë*, 12 maj 2015, Nr. 36862/05 lidhur me një konfiskim të aplikuar në procedurat civile; GJEDNJ, *Balsamo kundër San Marinos*, 8 tetor 2019, Nr. 20319/17 dhe 21414/17 në lidhje me procedurat e pastrimit të parave.

77 GJEDNJ, *Milorad Ulemek kundër Serbisë*, 2 shkurt 2021, Nr. 41680/13.

78 GJEDNJ, *Phillips kundër Mbretërisë së Bashkuar*, 5 korrik 2001, Nr. 41087/98; GJEDNJ, *Welch kundër Mbretërisë së Bashkuar*, 9 shkurt 1995, Nr. 17440/90; GJEDNJ, *Silickienė kundër Lituanisë*, 10 prill 2012, Nr. 20496/02; GJEDNJ, *Gogitidze dhe të tjerë kundër Gjeorgjisë*, 12 maj 2015, Nr. 36862/05.

- Prona që ka qenë objekt i veprës penale;⁷⁹
- Pronë që kishte shërbyer, ose ishte menduar të shërbente, për kryerjen e krimit.⁸⁰

Sa mund të sekuestrohet nga policia dhe të konfiskohet nga një gjykatë varet nga regjimi kombëtar i konfiskimit, i cili mund të zbatohet edhe për asetet virtuale në një çështje penale individuale.

GJEDNJ-ja ka shqyrtuar disa raste që trajtojnë proporcionalitetin dhe procesin e rregullt në procedurat e konfiskimit. Në çështjen *Todorov dhe të tjerët kundër Bullgarisë*,⁸¹ Gjykata vendosi se kishte pasur shkelje të nenit 1 të Protokollit 1 të KEDNJ-së në katër nga shtatë kërkesa. Gjykatat brenda vendit nuk kishin arritur të vendosnin një lidhje midis mallit të konfiskuar dhe veprimtarisë kriminale, ose midis vlerës së pasurisë dhe diferencës ndërmjet të ardhurave dhe shpenzimeve. Në këtë mënyrë, urdhri i konfiskimit kishte qenë jo proporcional.

Në *Balsamo kundër San Marino*,⁸² Gjykata pranoi se masat e konfiskimit ishin proporcionale, edhe në mungesë të një dënimi që vërteton fajësinë e të akuzuarit dhe nëse vendosej gjithashtu mbi fëmijët për shkak të precedentit të mëparshëm penal të babait të tyre. Për testin e proporcionalitetit, probabiliteti i lartë i origjinës së paligjshme, i kombinuar me paaftësinë e pronarit për të provuar të kundërtën, u konsiderua i mjaftueshëm.

Çështja *Gogitidze dhe të Tjerët kundër Gjeorgjisë*⁸³ kishte të bënte me një masë të vendosur nga gjykata të konfiskimit të pronës që i përkiste një ish-zëvendës ministri të Brendshëm. Gjykata konstatoi se ishte arritur një ekuilibër i drejtë ndërmjet mjeteve të përdorura për konfiskimin e pasurive të kërkuësve dhe interesit të përgjithshëm për të luftuar korrupsionin në shërbimin publik. Kërkuësve nuk iu është mohuar një mundësi e arsyeshme për të paraqitur çështjen e tyre dhe interpretimet e gjykatave brenda vendit nuk kanë qenë arbitrare.

79 GJEDNJ, *Agosi kundër Mbretërisë së Bashkuar*, 24 tetor 1986, Nr. 9118/80.

80 GJEDNJ, *Andonoski kundër ish Republikës Jugosllave të Maqedonisë*, 17 shtator 2015, Nr. 14464/11; GJEDNJ, *Todorov dhe të tjerë kundër Bullgarisë*, 13 korrik 2021, Nr. 50705/11 dhe 6 të tjerë.

81 GJEDNJ, *Todorov dhe të tjerë kundër Bullgarisë*, 13 korrik 2021, Nr. 50705/11 dhe 6 të tjerë.

82 GJEDNJ, *Balsamo kundër San Marinos*, 8 tetor 2019, Nr. 20319/17 dhe 21414/17.

83 GJEDNJ, *Gogitidze dhe të tjerë kundër Gjeorgjisë*, 12 maj 2015, Nr. 36862/05.

6

Përfundime



Respektimi i të drejtave të njeriut dhe sundimi i ligjit është një aspekt i rëndësishëm i çdo shoqërie demokratike dhe gjithashtu mund të jetë kusht për ligjshmërinë e provave dhe drejtësinë e një procedimi penal. Ajo gjithashtu ndikon në besimin që qytetarët kanë në institucionet publike dhe në shumë raste është një parakusht për sigurimin e bashkëpunimit ndërkombëtar që është kritik për hetime efektive të krimit kibernetik. Prandaj është e rëndësishme që profesionistët e drejtësisë penale të njohin dhe kuptojnë standardet e të drejtave të njeriut që zbatohen në fazat dhe proceset e ndryshme të një hetimi të krimit kibernetik.

Shumë të drejta të njeriut, duke përfshirë të drejtat për privatësi, një gjykim të drejtë, lirinë e shprehjes dhe mbrojtjen e pronës, mund të preken gjatë hetimeve të krimit kibernetik. Çdo ndërhyrje në të drejtat e njeriut që lejon kufizime në rrjedhën e hetimeve të krimit kibernetik duhet të **bazohet në ligj, të domosdoshëm dhe proporcional**, dhe të ndjekë një **qëllim legjitim**, siç është mbrojtja e të drejtave të njeriut të viktimave ose interesave të tjera të shoqërisë.

Standardet ndërkombëtare dhe rajonale të të drejtave të njeriut, si dhe jurisprudenca e gjykatave ndërkombëtare si GJEDNJ-ja, ofrojnë udhëzime të rëndësishme për Shtetet se si të zbatojnë në praktikë detyrimet e tyre për të drejtat e njeriut në lidhje me hetimet e krimit kibernetik. Kjo përfshin themelimin e legjislacionit vendas për të rregulluar përdorimin e kompetencave hetuese në përputhje me standardet dhe masat mbrojtëse ndërkombëtare të të drejtave të njeriut, dhe sigurimin që profesionistët kanë njohuritë dhe aftësitë e nevojshme për të mbështetur këto standarde gjatë hetimeve të krimit kibernetik.

7

Shtojcat



SHTOJCA 1 NENET PËRKATËSE TË ICCPR-SË DHE KEDNJ-SË
SHTOJCA 2 JURISPRUDENCA E PËRZGJEDHUR E GJEDNJ-SË

SHTOJCA 1

NENET PËRKATËSE TË ICCPR-SË DHE KEDNJ-SË

E DREJTA PËR TË RESPEKTUAR JETËN PRIVATE DHE FAMILJARE

ICCPR Neni 17

1. Askush nuk duhet t'i nënshtrohet ndërhyrjeve arbitrare ose të paligjshme në privatësinë, familjen, shtëpinë ose korrespondencën e tij, as sulmeve të paligjshme ndaj nderit dhe reputacionit të tij.
2. Gjithkush ka të drejtën e mbrojtjes me ligj kundër ndërhyrjeve apo sulmeve të tilla.

KEDNJ Neni 8

1. Secili ka të drejtën e respektimit të jetës së tij private dhe familjare, shtëpisë dhe korrespondencës së tij.
2. Nuk ka asnjë ndërhyrje nga një autoritet publik në zbatimin e kësaj të drejte, përveç asaj që është në përputhje me ligjin dhe është e nevojshme në një shoqëri demokratike në interes të sigurisë kombëtare, sigurisë publike ose mirëqenies ekonomike të vendit, për parandalimin e çrregullimit ose krimit, për mbrojtjen e shëndetit ose moralit, ose për mbrojtjen e të drejtave dhe lirive të të tjerëve.

E DREJTA PËR NJË GJYKIM TË DREJTË

ICCPR Neni 14

1. Të gjithë personat janë të barabartë para gjykatave dhe tribunaleve. Në përcaktimin e çdo akuze penale kundër tij, ose për të drejtat dhe detyrimet e tij në një padi, secili gëzon të drejtën e një gjykimi të drejtë dhe publik nga një gjykatë kompetente, e pavarur dhe e paanshme e krijuar me ligj. Shtypi dhe publiku mund të përjashtohen nga i gjithë ose një pjesë e një gjyqi për arsye morali, rendit publik ose sigurisë kombëtare në një shoqëri demokratike, ose kur këtë e kërkon interesi i jetës private të palëve, ose masën rreptësishtë të nevojshme sipas mendimit të gjykatës në rrethana të veçanta ku publiciteti do të cenonte interesat e drejtësisë; por çdo gjykim i dhënë në një çështje penale ose në një padi bëhet publik, përveç rasteve kur interesi i personave të mitur kërkon ndryshe ose kur procedimet kanë të bëjnë me mosmarrëveshjet martesore ose kujdestarinë e fëmijëve.
2. Secili i akuzuar për një vepër penale gëzon të drejtën të konsiderohet i pafajshëm derisa të provohet fajësia e tij sipas ligjit.
3. Në përcaktimin e çdo akuze penale kundër tij, çdokush gëzon të drejtën e garancive minimale në vijim, në barazi të plotë:
 - a. Të informohet menjëherë dhe me hollësi në një gjuhë që ai kupton për llojin dhe shkakun e akuzës kundër tij;
 - b. Të ketë kohën dhe lehtësitë e duhura për përgatitjen e mbrojtjes së tij dhe për të komunikuar me avokatin e zgjedhur prej tij;

- c. Të gjykohet pa vonesa të panevojshme;
 - d. Të gjykohet në praninë e tij dhe të mbrohet personalisht ose nëpërmjet ndihmës juridike të zgjedhur prej tij; të informohet, nëse nuk ka ndihmë juridike, për këtë të drejtë; dhe t'i caktohet asistenca juridike, në çdo rast kur këtë e kërkojnë interesat e drejtësisë, dhe pa pagesë prej tij në çdo rast, nëse nuk ka mjete të mjaftueshme për ta paguar atë;
 - e. Të marrë në pyetje ose të ketë marrë në pyetje dëshmitarët kundër tij dhe të sigurojë pjesëmarrjen dhe marrjen në pyetje të dëshmitarëve në emër të tij në të njëjtat kushte si dëshmitarët kundër tij;
 - f. Të ketë e një përkthyesi pa pagesë nëse nuk kupton ose nuk flet gjuhën e përdorur në gjykatë;
 - g. Të mos detyrohet të dëshmojë kundër vetes ose të pranojë fajësinë.
4. Në rastin e personave të mitur, procedura duhet të jetë e tillë që do të marrë parasysh moshën e tyre dhe dëshirën për të përkrahur rehabilitimin e tyre.
 5. Çdokush i dënuar për një krim gëzon të drejtën që vendimi dhe dënimi i tij të rishqyrtohen nga një gjykatë më e lartë sipas ligjit.
 6. Kur një person është dënuar me vendim të formës së prerë për një vepër penale dhe më pas i është anuluar dënimi ose është falur me arsyetimin se një fakt i ri ose i zbuluar rishtazi tregon përfundimisht se ka pasur një shkelje të drejtësisë, personi i cili ka vuajtur dënimin si pasojë e këtij dënimi shpërblehet sipas ligjit, përveç nëse vërtetohet se moszbulimi në kohë i faktit të panjohur i atribuohet në mënyrë të plotë ose të pjesëshme atij.
 7. Askush nuk mban përgjegjësi për t'u gjykuar ose ndëshkuar përsëri për një vepër për të cilën personi tashmë është dënuar përfundimisht ose shpallur i pafajshëm në përputhje me ligjin dhe procedurën penale të çdo vendi.

KEDNJ Neni 6

1. Në përcaktimin e të drejtave dhe detyrimeve të tij civile ose për çdo akuzë penale kundër tij, çdokush ka të drejtën e një gjykimi të drejtë dhe publik brenda një kohe të arsyeshme nga një gjykatë e pavarur dhe e paanshme e themeluar me ligj. Vendimi shpallet publikisht, por shtypi dhe publiku mund të përjashtohen nga i gjithë ose një pjesë e gjykimit në interes të moralit, rendit publik ose sigurisë kombëtare në një shoqëri demokratike, ku interesat e të miturve ose mbrojtja e jetës private në interes të palëve, ose në masën rreptësishtë të nevojshme sipas gjykimit të gjykatës në rrethana të veçanta kur publiciteti do të cenonte interesat e drejtësisë.
2. Kushdo që akuzohet për një vepër penale konsiderohet i pafajshëm derisa të provohet fajësia e tij sipas ligjit.
3. Çdo person i akuzuar për një vepër penale gëzon këto të drejta minimale:
 - a. Të informohet menjëherë, në një gjuhë që ai e kupton dhe në detaje, për llojin dhe shkakun e akuzës kundër tij;
 - b. Të ketë kohë dhe lehtësitë e mjaftueshme për përgatitjen e mbrojtjes së tij;
 - c. Të mbrohet personalisht ose nëpërmjet ndihmës juridike të zgjedhur prej tij ose, nëse nuk ka mjete të mjaftueshme për të paguar ndihmën juridike, t'i jepet falas kur këtë e kërkojnë interesat e drejtësisë;
 - d. Të marrë në pyetje ose të ketë marrë në pyetje dëshmitarët kundër tij dhe të sigurojë

pjesëmarrjen dhe marrjen në pyetje të dëshmitarëve në emër të tij në të njëjtat kushte si dëshmitarët kundër tij;

- e. Të ketë ndihmën e një përkthyesi pa pagesë nëse nuk kupton ose nuk flet gjuhën e përdorur në gjykatë.

LIRIA E SHPREHJES

ICCPR Neni 19

1. Gjithkush ka të drejtë të japë mendime pa ndërhyrje.
2. Çdokush ka të drejtën e lirisë së shprehjes; kjo e drejtë do të përfshijë lirinë për të kërkuar, marrë dhe dhënë informacione dhe ide të të gjitha llojeve, pavarësisht kufijve, qoftë gojarisht, me shkrim ose në shtyp, në formën e artit ose nëpërmjet çdo mjeti tjetër sipas zgjedhjes së tij.
3. Zbatimi i të drejtave të parashikuara në pikën 2 të këtij neni mbart me vete detyra dhe përgjegjësi të veçanta. Prandaj mund t'i nënshtrohet kufizimeve të caktuara, por këto do të jenë vetëm ato që parashikohen me ligj dhe janë të nevojshme:
 - a. Për respektimin e të drejtave ose reputacionit të të tjerëve;
 - b. Për mbrojtjen e sigurisë kombëtare ose të rendit publik, ose të shëndetit ose moralit publik.

KEDNJ Neni 10

1. Gjithkush ka të drejtën e lirisë së shprehjes. Kjo e drejtë përfshin lirinë për të mbajtur opinione dhe për të marrë e për të dhënë informacione dhe ide pa ndërhyrje nga autoriteti publik dhe pavarësisht kufijve. Ky nen nuk i pengon Shtetet që të kërkojnë licencimin e ndërmarreve të transmetimit, televizionit ose kinemasë.
2. Ushtrimi i këtyre lirive, duke qenë se mbart me vete detyra dhe përgjegjësi, mund t'i nënshtrohet formaliteteve, kushteve, kufizimeve ose gjobave të përcaktuara me ligj dhe që janë të nevojshme në një shoqëri demokratike, në interes të sigurisë kombëtare, integritetit territorial ose sigurinë publike, për parandalimin e çrregullimeve ose krimeve, për mbrojtjen e shëndetit ose moralit, për mbrojtjen e reputacionit ose të drejtave të të tjerëve, për parandalimin e zbulimit të informacionit të marrë në mënyrë konfidenciale, ose për ruajtjen e autoritetit dhe paanshmërisë së gjyqësorit.

E DREJTA PËR MBROJTJEN E PRONËS

Neni 1 i Protokollit 1 të KEDNJ-së

1. Çdo person fizik ose juridik gëzon të drejtën e zotërimit të qetë të pronës së tij. Askush nuk mund të privohet nga pronat e tij, përveçse për interesin publik dhe në varësi të kushteve të parashikuara nga ligji dhe nga parimet e përgjithshme të së drejtës ndërkombëtare.
2. Megjithatë, dispozitat e lartpërmendura nuk do të cenojnë në asnjë mënyrë të drejtën e një shteti për të zbatuar këto ligje që ai i sheh të nevojshme për të kontrolluar përdorimin e pronës në përputhje me interesin e përgjithshëm ose për të siguruar pagesën e taksave, kontributeve ose gjobave të tjera.

SHTOJCA 2

JURISPRUDENCA E PËRZGJEDHUR E GJEDNJ-SË

Benedik kundër Sllovenisë⁸⁴

Çështja kishte të bënte me shkeljen e të drejtës për respektimin e jetës private sipas Nenit 8 të KEDNJ-së. Në vitin 2006, policia sllovene mori informacion nga policia zvicerane lidhur me një shkëmbim dosjesh që përmbanin pornografi për fëmijë nëpërmjet një faqe interneti për ndarjen e skedarëve homologë. Ndërmjet adresave IP të regjistruara nga policia zvicerane ishte një adresë dinamike IP në Slloveni. Në gusht 2006, policia sllovene, pa një urdhër gjyqate, i kërkoi një ofruesi të shërbimit të internetit (ISP) me bazë në Slloveni të zbulonte të dhënat për një përdorues të cilit i ishte caktuar adresa dinamike IP në një kohë të caktuar. Kërkesa bazohej në dispozitën e Ligjit të Procedurës Penale që i lejonte policisë të kërkonte informacion nga një ofrues i komunikimit elektronik për përdoruesit e një mjeti të caktuar të komunikimit elektronik, të dhënat e të cilit nuk ishin të disponueshme në drejtorinë përkatëse.

ISP-ja siguroi emrin dhe adresën e abonentit lidhur me adresën përkatëse IP. Më pas, në dhjetor 2006, u lëshua një urdhër gjyqate që i kërkoi ISP-së të zbulojë të dhënat personale dhe të dhënat e trafikut të abonentit që lidhet me adresën IP në fjalë. Në bazë të të dhënave të marra, një gjykatë rrethi urdhëroi një kontroll në shtëpinë e familjes së kërkuesit në janar 2007. Gjatë kontrollit, u sekuestruan kompjuterë me materiale pornografike me të mitur.

Në dhjetor 2008, kërkuesi u shpall fajtor për veprën penale të shfaqjes, prodhimit, zotërimit dhe shpërndarjes së materialeve pornografike. Ai u dënua me burgim me kusht prej tetë muajsh me një periudhë prove prej dy vitesh. Në nëntor 2009, në apel, Gjykata e Lartë e Lubjanës e ktheu dënimin me kusht të kërkuesit në një burgim prej gjashtë muajsh.

Kërkuesi pa sukses ndoqi rekursin ligjor përpara gjykatave brenda vendit, duke pretenduar se privatësia e korrespondencës dhe mjeteve të tjera të komunikimit mund të pezullohej vetëm në bazë të një vendimi gjyqësor dhe për këtë arsye çdo informacion i marrë në mënyrë të paligjshme duhet të përjashtohet si provë. Ankesa e kërkuesit kishte të bënte me kërkesën e parë të policisë drejtuar ISP-së për identifikimin e përdoruesit të adresës IP në bazë të Aktit të Procedurës Penale.

Në këtë drejtim, Gjykata Kushtetuese vendosi në shkurt 2014 se Kushtetuta mbronte edhe të dhënat e trafikut, pra çdo të dhënë të përpunuar për transmetimin e komunikimeve në një rrjet të komunikimeve elektronike. Mori parasysh se adresat IP përfshiheshin në të dhënat e tilla të trafikut dhe se normalisht do të kërkoheshin një urdhër gjyqate. Megjithatë, kërkuesi, i cili nuk e kishte fshehur në asnjë mënyrë adresën IP nëpërmjet së cilës kishte hyrë në internet, ishte ekspozuar me vetëdije ndaj publikut dhe kishte hequr dorë nga pritshmëria e ligjshme e privatësisë. Si rezultat, megjithëse të dhënat lidhur me identitetin e përdoruesit të adresës IP mbroheshin në parim si privatësi komunikimi sipas Kushtetutës, Gjykata Kushtetuese vendosi se nuk kërkoheshin asnjë urdhër gjyqate për t'i zbuluar ato në rastin e kërkuesit.

Kur çështja u dërgua në GJEDNJ, Gjykata arriti në përfundimin se kërkesa e policisë drejtuar

84 GJEDNJ, *Benedik kundër Sllovenisë*, 24 prill 2018, Nr. 62357/14; përmbledhur në: GJEDNJ, Shënim informues për çështjen gjyqësore të Gjykatës 217.

ISP-së dhe përdorimi i informacionit të abonentit që çoi në identifikimin e kërkuesit kishte çuar në ndërhyrje në të drejtat e tij sipas Nenit 8 të KEDNJ-së. Gjykata vuri në dukje se masat e policisë kishin një bazë në ligjin e brendshëm. Duke qenë se legjislacioni përkatës nuk ishte koherent lidhur me nivelin e mbrojtjes që i jepej interesit të privatësisë së kërkuesit, Gjykata u mbështet në interpretimin e Gjykatës Kushtetuese, sipas të cilit zbulimi i informacionit të abonentit që lidhet me një adresë IP të caktuar dinamike kërkonte në parim një urdhër gjykatë, pasi të dhënat e trafikut binin në mbrojtje të Kushtetutës. Për sa i përket qëndrimit të Gjykatës Kushtetuese se kërkuesi në çështjen konkrete kishte hequr dorë nga pritshmëria e ligjshme e privatësisë pasi nuk kishte fshehur në asnjë mënyrë adresën IP përmes së cilës kishte akses në internet, GJEDNJ-ja nuk e konstatoi atë në pajtim me qëllimin e të drejtës për privatësi sipas KEDNJ-së. Prandaj, një urdhër gjykatë ishte i nevojshëm në rastin konkret dhe asnjë gjë në ligjin e brendshëm nuk e pengonte policinë ta merrte atë.

GJEDNJ-ja krijoi legjislacionin, përkatësisht dispozitat përkatëse të Ligjit të Procedurës Penale (që nuk përmbante rregulla specifike për lidhjen ndërmjet adresës dinamike IP dhe informacionit të abonentit), Ligjit të Komunikimeve Elektronike (i cili rregullonte në mënyrë specifike sekretin dhe konfidencialitetin e komunikimit elektronik), dhe Kushtetuta (e cila kërkonte një urdhër gjykatë për çdo ndërhyrje në privatësinë e komunikimit), jo koherente për nivelin e mbrojtjes që i ofrohet interesit të privatësisë së kërkuesit.

Në këtë kontekst, Gjykata gjithashtu theksoi se, në kohën e duhur, nuk kishte asnjë rregullore që specifikonte kushtet për ruajtjen e të dhënave të marra sipas Ligjit të Procedurës Penale dhe se procedura për aksesin dhe transmetimin e këtyre të dhënave nuk përmbante masa mbrojtëse kundër abuzimit nga Zyrtarët e shtetit. Asnjë mbikëqyrje e pavarur e përdorimit të kompetencave policore lidhur me marrjen e informacionit nga ISP-të nuk kishte ekzistuar në kohën e duhur.

Rrjedhimisht, GJEDNJ-ja arriti në përfundimin se ligji mbi të cilin bazohej masa e kontestuar dhe mënyra se si u zbatua nga gjykatat e vendit nuk kishte qartësi dhe nuk ofronte masa mbrojtëse të mjaftueshme kundër ndërhyrjeve arbitrare në Nenin 8 të KEDNJ-së. Gjykata konstatoi se ndërhyrja në të drejtën e kërkuesit për respektimin e jetës së tij private nuk ishte “në përputhje me ligjin”, siç kërkohet nga Neni 8 (2) i Konventës.

Pas vendimit, policia dhe prokurorët slovenë ndryshuan praktikën e tyre menjëherë. Në vitin 2019, Ligji i Procedurës Penale u ndryshua për të specifikuar se të dhënat e abonentëve mund të merren pa urdhër gjykatë vetëm nëse nuk analizohen të dhënat e trafikut. Në praktikë, kjo nënkupton se duhet një urdhër gjykatë për të hyrë në të dhënat e përdoruesit të një adrese IP specifike dinamike. Ky nuk është rasti kur të dhënat e abonentit përfshihen në një kontratë me një ofrues shërbimi, për shembull për një numër telefoni celular ose një adresë të pandryshueshme IP.

Në qershor 2018, z. Benedik ka paraqitur kërkesë për mbrojtjen e ligjshmërisë pranë Gjykatës së Lartë. Në qershor 2020, Gjykata e Lartë miratoi kërkesën e kërkuesit për mbrojtjen e ligjshmërisë, anuloi vendimin përfundimtar dhe e ktheu çështjen në Gjykatën e Rrethit Kranj për rigjykim. Në maj 2021, Gjykata e Rrethit Kranj ndërpriti procedurën penale kundër z. Benedik pasi Prokuroria e Qarkut Kranj tërhoqi padinë.

Si përfundim, duhet theksuar se kushti i një urdhri gjykatë për marrjen e të dhënave të përdoruesit të një adrese IP (dinamike) buron nga Kushtetuta slovene dhe jurisprudenca e Gjykatës Kushtetuese slovene dhe nuk është një standard ndërkombëtar. Çështja tregon gjithashtu rëndësinë e së drejtës për respektimin e jetës private dhe qartësisë së mjaftueshme ligjore dhe

praktikës së përshtatshme kur ndërhyhet në të drejtat e njeriut. Për shkak të shkeljes së KEDNJ-së në këtë rast, provat digjitale janë përjashtuar dhe procedura e rinovuar penale është ndërprerë.

Breyer kundër Gjermanisë⁸⁵

Sipas ndryshimeve të vitit 2004 në Aktin Gjerman të Telekomunikacionit, shoqërive të telekomunikacionit u kërkohet të mbledhin dhe ruanin të dhënat personale të të gjithë klientëve të tyre, duke përfshirë përdoruesit e kartave SIM me parapagesë, edhe kur nuk ishte e nevojshme për qëllime faturimi ose arsye të tjera kontraktore, dhe t'i vinin ato në dispozicion të autoriteteve sipas kërkesës. Klientët duhet të regjistrojnë të dhënat personale si emrin dhe adresën e tyre, numrat e telefonit dhe datën e lindjes me ofruesit e tyre të shërbimeve. Ata u ankuan për ruajtjen e të dhënave të tyre personale si përdorues të kartave SIM me parapagesë.

GJEDNJ-ja u shpreh se nuk kishte pasur shkelje të Nenit 8 të KEDNJ-së (e drejta për respektimin e jetës private). Gjykata konstatoi se, përgjithësisht, Gjermania nuk i kishte tejkaluar kufijtë e gjykimit të saj (“kufiri i vlerësimit”) në zgjedhjen e mjeteve për të arritur qëllimet e ligjshme të mbrojtjes së sigurisë kombëtare dhe luftimit të krimit, dhe se ruajtja e të dhënave personale të kërkuesve kanë qenë të barabarta dhe “të nevojshme në një shoqëri demokratike”. Si rrjedhojë, nuk kishte pasur shkelje të Konventës.

Veçanërisht, Gjykata konstatoi se mbledhja e emrave dhe adresave të kërkuesve si përdorues të kartave SIM me parapagesë përbënte një ndërhyrje të kufizuar në të drejtat e tyre. Megjithatë, gjykata vuri në dukje se ligji në fjalë kishte masa mbrojtëse shtesë dhe se njerëzit gjithashtu mund t'u drejtoheshin organeve të pavarura të mbikëqyrjes së të dhënave për të shqyrtuar kërkesat e autoriteteve për të dhënat dhe për të kërkuar korrigjim ligjor nëse është e nevojshme.

Lidhur me përdorimin e të dhënave të ruajtura, të dhënat mund të kërkohen nga autoritete të ndryshme publike pa pasur nevojë për një urdhër gjykatë ose njoftim të personave në fjalë. Kërkesat për marrjen e të dhënave në kushte të caktuara mund të automatizohen dhe të rezultojnë në lista të bazuara në ngjashmëri të thjeshtë (pyetje të të dhënave të pjeshme) në emra ose numra. Kërkesat për informacion ishin të lejueshme kur konsiderohej e nevojshme “për të ndjekur penalisht vepra penale dhe administrative, për të shmangur rrezikun dhe për të kryer detyrat e inteligjencës”.

Veçanërisht, Gjykata shqyrtoi dy aspekte kryesore. Së pari, nëse ndërhyrja ishte e nevojshme në një shoqëri demokratike dhe të barabartë, duke përfshirë çështjen e parashikueshmërisë dhe detajeve të mjaftueshme të dispozitave përkatëse. Gjykata pranoi se ruajtja në fjalë ishte, nga një këndvështrim i përgjithshëm, një përgjigje e përshtatshme ndaj ndryshimeve në sjelljen e komunikimit dhe në mjetet e telekomunikacionit:

- Regjistrimi paraprak i abonentëve të telefonit celulare e bëri më të thjeshtë dhe përshejtoi më shumë hetimin nga autoritetet e zbatimit të ligjit dhe në këtë mënyrë mund të kontribuojë në zbatimin efektiv të ligjit dhe parandalimin e trazirave ose krimit.
- Ekzistenca e mundësive për të shmangur detyrimet ligjore nuk mund të jetë një arsye për të

85 GJEDNJ, *Breyer kundër Gjermanisë*, 30 janar 2020, Nr. 50001/12; përmbledhur në: GJEDNJ, Shënim informues për çështjen gjyqësore 236 të Gjykatës.

vënë në pikëpyetje dobinë dhe efektivitetin e tyre të përgjithshëm.

- Përveç mungesës së konsensusit, fakti që shqetësimet për sigurinë kombëtare ishin në rrezik justifikonte edhe një kufi të caktuar vlerësimi.

Aspekti i dytë që trajtohet nga Gjykata kishte të bënte me çështjen nëse ndërhyrja në të drejtën e jetës private ishte e barabartë. Ndryshe nga rastet e shqyrtuara më parë nga Gjykata, ruajtja e të dhënave në fjalë nuk përfshinte ndonjë informacion tepër personal ose nuk lejonte krijimin e profileve të personalitetit ose gjurmimin e lëvizjeve të abonentëve. Gjithashtu, nuk u ruajtën të dhëna që lidhen me rastet individuale të komunikimit. Edhe pse e rëndësishme, ndërhyrja në këtë mënyrë ishte mjaft e kufizuar në natyrë.

Për sa i përket masave mbrojtëse lidhur me regjistrimin dhe ruajtjen e të dhënave në mënyrë individuale, Gjykata theksoi se:

- Kërkuesit nuk kishin pretenduar se kjo ruajtje kishte qenë subjekt i ndonjë pasigurie teknike.
- Kohëzgjatja e ruajtjes ishte e kufizuar në vitin kalendarik pas vitit në të cilin kishte përfunduar marrëdhënia kontraktore; kjo nuk dukej e tepruar, duke qenë se hetimet për veprat penale mund të zgjasin pak dhe të shtriheshin përtej përfundimit të marrëdhënies kontraktore.
- Të dhënat e ruajtura ishin kufizuar në informacionin e nevojshëm për të identifikuar qartë abonentin përkatës.
- Kërkesat e automatizuara sipas Aktit të Telekomunikacionit janë të kufizuara në autoritete specifike në fushën e zbatimit të ligjit dhe sigurisë kombëtare. Kërkesat manuale, nga ana tjetër, nuk janë renditur qartësisht, por përcaktohen në bazë të detyrave të autoriteteve (p.sh., parandalimi i rreziqeve, ndjekja penale e krimeve, zbatimi i rregulloreve). Ky nivel detajesh është i përshtatshëm, pavarësisht mungesës së një numërimi të qartë të autoriteteve në fjalë.

Gjykata Kushtetuese Federale Gjermane shqyrtoi gjithashtu çështjen nëse kishte masa mbrojtëse të mjaftueshme për aksesin e mundshëm në të ardhmen dhe përdorimin e të dhënave të ruajtura, veçanërisht lidhur me aspektet në vijim:

- Kompetenca për lëshimin e kërkesave për informacion: fakti që ligji ekzistues përcakton se informacioni mund të jepet vetëm për aq sa është i nevojshëm për kryerjen e detyrës, krijon tashmë në mënyrë objektive një faktor kufizues. Kjo siguron që marrjet e të dhënave të lejohen vetëm kur informacioni i nevojshëm për kryerjen e detyrave nuk mund të merret më lehtë, por në një mënyrë tjetër po aq efektive. Si rrjedhojë, nuk ka asnjë kërkesë në nivel jo kushtetues që autoritetet e autorizuara ta specifikojnë shprehimisht me ligj.
- Qëllimi i kërkesave për informacion: autoritetet kërkuese duhej të kishin një bazë ligjore shtesë për të marrë të dhënat (analogjia e sistemit me portë të dyfishtë⁸⁶).
- Shtrirja e kërkesave për informacion: marrja e të dhënave ishte e kufizuar në të dhënat e nevojshme sipas një detyrimi të përgjithshëm për të fshirë çdo të dhënë që autoritetit kërkues nuk i duheshin pa vonesa të panevojshme. Për më tepër, kërkesa e “nevojës” nuk ishte e natyrshme vetëm në dispozitat ligjore specifike në varësi të kësaj ankese, por edhe në ligjin gjerman dhe evropian për mbrojtjen e të dhënave.

86 Një shkëmbim i të dhënave bëhet ndërmjet ndërhyrjeve të marrjes dhe transferimit, të cilat korrespondojnë me njëra-tjetrën dhe secila prej tyre kërkon një bazë ligjore të pavarur. E thënë në mënyrë figurative, organi ligjvënës duhet të hapë jo vetëm derën për transmetimin e të dhënave, por edhe derën për marrjen e tyre. Janë vetëm të dyja bazat ligjore së bashku, të cilat duhet të funksionojnë së bashku si një portë e dyfishtë, të cilat i japin autoritetet shkëmbimit të të dhënave personale.

- Rishikimi dhe mbikëqyrja e kërkesave për informacion: edhe nëse përgjegjësia për ligjshmërinë e kërkesës së informacionit binte mbi vetë agjencitë e marrjes, Agjencia Federale e Rrjetit u konsiderua e përshtatshme për të shqyrtuar në mënyrë të pavarur pranimin e transmetimit të të dhënave kur e shihte të arsyeshme për të vepruar kështu. Gjithashtu, korrigjimi ligjor kundër marrjes së informacionit mund të kërkohet sipas rregullave të përgjithshme. Duke marrë parasysh këto rrugë për rishikim, mungesa e njoftimit për procedurën e marrjes së të dhënave nuk ngriti një çështje sipas Konventës.

GJEDNJ-ja konfirmoi vendimin e Gjykatës Kushtetuese Federale Gjermane se nuk kishte pasur shkelje të të drejtave të njeriut dhe theksoi rëndësinë e kufizimeve ligjore dhe masave mbrojtëse në kuadrin e kufirit kombëtar të vlerësimit për të përmbushur parimet e proporcionalitetit dhe nevojës në një shoqëri demokratike. Në mënyrë të veçantë, gjykata konstatoi se detyrimi ligjor i ofruesve të shërbimeve për të ruajtur të dhënat personale të përdoruesve të kartave SIM të telefonit celular me parapagesë dhe për t'i vënë ato në dispozicion të autoriteteve sipas kërkesës ishte në proporcion me qëllimet e ligjshme të mbrojtjes së sigurisë kombëtare dhe luftimit të krimit, dhe se marrja e të dhënave nga autoritetet u shoqërua me masa mbrojtëse të përshtatshme.

Roman Zakharov kundër Ruisë⁸⁷

Kërkuesi, i cili ishte kryeredaktor i një shoqërie botuese, ngriti procedim gjyqësor kundër tre operatorëve të rrjetit celular, duke u ankuar për ndërhyrje në të drejtën e tij për privatësinë e bisedave të tij telefonike. Ai pretendoi se, në përputhje me ligjin e brendshëm përkatës, operatorët e rrjetit celular kishin instaluar pajisje të cilat i mundësonin Shërbimit Federal të Sigurisë të përgjonte të gjitha bisedat telefonike pa autorizim paraprak gjyqësor. Ai kërkoi një urdhër për heqjen e pajisjeve dhe për t'u siguruar që aksesit në telekomunikacion t'i jepej vetëm personelit të autorizuar.

Gjykatat brenda vendit hodhën poshtë pretendimin e kërkuesit, duke konstatuar se ai nuk kishte arritur të vërtetonte se bisedat e tij telefonike ishin përgjuar ose se operatorët celularë kishin transmetuar informacion të mbrojtur ndaj personave të paautorizuar. Gjykatat vendase konstatuan gjithashtu se instalimi i pajisjeve të cilave iu referua kërkuesi nuk cenonte në vetvete privatësinë e komunikimit të tij.

GJEDNJ-ja konstatoi se ekzistenca e thjeshtë e legjislacionit të kontestuar për përgjimin e komunikimeve të telefonit celular përbënte në vetvete një ndërhyrje në zbatimin e të drejtave të kërkuesit sipas Nenit 8. Gjykata shqyrtoi disa aspekte të ndërhyrjes në Nenin 8:

- **Ligjshmëria:** Përgjimi i komunikimeve të telefonit celular kishte bazë në ligjin e brendshëm dhe ndiqte qëllimet e ligjshme të mbrojtjes së sigurisë kombëtare dhe publike, parandalimin e krimit dhe mbrojtjen e mirëqenies ekonomike të vendit.
- **Aksesi:** dispozitat ligjore ishin publikuar zyrtarisht dhe ishin të aksesueshme për publikun.
- **Fusha e zbatimit të masave të mbikëqyrjes sekrete:** lloji i veprave penale që mund të shkaktonte një urdhër përgjimi ishte mjaft i qartë. Megjithatë, shtrirja ishte shumë e gjerë dhe

87 GJEDNJ, *Roman Zakharov kundër Ruisë*, 4 dhjetor 2015, Nr. 47143/06; përmbledhur në: GJEDNJ, Shënim informues për çështjen gjyqësore të Gjykatës 191.

përgjimi mund të urdhërohej jo vetëm për individët që ishin të dyshuar ose të akuzuar.

- **Kohëzgjatja e masave të mbikëqyrjes sekrete:** ligji përmbante rregulla të qarta për kohëzgjatjen dhe rinovimin e përgjimeve, por jo për ndërprerjen e përgjimeve.
- **Procedurat,** ndër të tjera, për ruajtjen dhe shkatërrimin e të dhënave të përgjuara: ruajtja automatike për gjashtë muaj e të dhënave qartësisht të parëndësishme nuk mund të konsiderohet e justifikuar sipas Nenit 8.
- **Autorizimi i përgjimeve:** Përgjimi duhej të autorizohet nga një gjykatë, por gjyqtarët rusë nuk u udhëzuan të verifikonin ekzistencën e “dyshimit të arsyeshëm” përkundrejt personit në fjalë ose të zbatonin testet e “nevojës” dhe “proporcionalitetit”. Ligji nuk përmbante asnjë kërkesë lidhur me përmbajtjen e kërkesave apo autorizimeve për përgjim. Disa urdhra nuk përmendin një person specifik apo numër telefoni apo kohëzgjatjen e mbikëqyrjes. Nuk kishte asnjë detyrim sipas ligjit të brendshëm për t'i treguar autorizimin gjyqësor ofruesit të shërbimit të komunikimit përpara se të merrte akses në komunikime.
- **Mbikëqyrja:** ishte e pamundur për autoritetin mbikëqyrës të zbulonte përgjimet e kryera pa autorizimin e duhur gjyqësor, i cili, i kombinuar me aftësinë teknike të autoriteteve të zbatimit të ligjit për të përgjuar drejtpërdrejt komunikimet, i bën marrëveshjet e mbikëqyrjes joefektive. Mbikëqyrja nga prokurorët ishte e kufizuar.
- **Njoftimi për përgjimin dhe mjetet gjyqësore të disponueshme:** personat, komunikimet e të cilëve u përgjuan nuk u njoftuan.

Mjetet gjyqësore të përdorura nga qeveria ishin në dispozicion vetëm për personat që zotëronin informacione për përgjimin e komunikimeve të tyre. Prandaj, efektiviteti i tyre u cenua nga mungesa e një kërkesë për të njoftuar personin që i nënshtrohet përgjimit ose nga një mundësi adekuate për të kërkuar dhe marrë informacion lidhur me përgjimin nga autoritetet. Prandaj, ligji Rus nuk parashikonte një mjet gjyqësor efektiv kundër masave të mbikëqyrjes sekrete në rastet kur nuk u ngrit asnjë procedim penal kundër personit që i nënshtrohej përgjimit.

Si të tilla, dispozitat ligjore vendase që rregullojnë përgjimin e komunikimeve nuk ofronin garanci adekuate dhe efektive kundër arbitraritetit dhe rrezikut të abuzimit. Ligji i brendshëm nuk plotësonte kërkesën e “cilësisë së ligjit” dhe ishte i paaftë që të kufizonte “ndërhyrjen” në atë që ishte “e nevojshme në një shoqëri demokratike”. Përmes gjykimit të saj, GJEDNJ vendosi standarde të sakta dhe një test përputhshmërie për legjislacionin në rastin e mbikëqyrjes masive.

K.U. kundër Finlandës⁸⁸

Në këtë rast, GJEDNJ diskutoi detyrimet pozitive të Shteteve Palë në lidhje me mbrojtjen efektive të jetës private (privatësisë) dhe përdorimin e të dhënave të komunikimit në rastet që lidhen me provat digjitale dhe krimin kibernetik. Rasti kishte të bënte me një djalë 12-vjeçar finlandez, të dhënat e të cilit u shpërndanë kundër dëshirës së tij në një faqe takimesh dhe të cilit iu afhua një i rritur. Është e qartë se një qasje e tillë (seksuale) ishte e paligjshme në atë kohë, veçanërisht pasi autori mbeti anonim.

Kur autoritetet finlandeze u përpoqën të ndiqnin penalisht çështjen, ata nuk mundën të merrnin

88 GJEDNJ, *K.U. kundër Finlandës*, 2 dhjetor 2008, Nr. 2872/02; përmbledhur në: GJEDNJ, Shënim informues për çështjen gjyqësore të GJykatës 114.

detajet e autorit nga ofruesi i shërbimit të faqes së takimeve. Ofruesi i shërbimit nuk ishte në gjendje sipas legjislacionit finlandez të zbulonte identitetin e përdoruesit me kërkesë të policisë. Gjykata vlerësoi këtë rezultat dhe konstatoi se ligjvënësi finlandez nuk kishte marrë masa të mjaftueshme për të trajtuar një situatë të tillë.

Në aktgjykim thuhet: “Gjykata vlerëson se mbrojtja praktike dhe efektive e kërkuesit kërkonte që të ndërmerren hapa efektivë për identifikimin dhe ndjekjen penale të autorit, pra personit që ka vendosur reklamën. Në rastin konkret, një mbrojtje e tillë nuk është ofruar. Një hetim efektiv nuk mund të nisë kurrë për shkak të një kërkesë mbizotëruese të konfidencialitetit.

Edhe pse liria e shprehjes dhe konfidencialiteti i komunikimeve janë konsideratat kryesore dhe përdoruesit e shërbimeve të telekomunikacionit dhe internetit duhet të kenë një garanci se do të respektohet privatësia e tyre dhe liria e shprehjes, një garanci e tillë nuk mund të jetë absolute dhe duhet t'i nënshtrohet me raste imperative të tjera legjitime, si p.sh., si parandalimi i çrregullimit ose krimit ose mbrojtja e të drejtave dhe lirive të tjerëve”.

Prandaj, Gjykata arriti në përfundimin se rasti i K.U. nuk mund të trajtohej në mënyrë efektive sipas kuadrit ligjor ekzistues, duke çuar në shkëlqen e detyrës pozitive të shtetit për të mbrojtur K.U. nga kjo lloj sjelljeje. Shteti kishte dështuar në mbrojtjen e të drejtës së K.U-së për respektimin e jetës së tij private, duke i dhënë përparësi kërkesës së konfidencialitetit mbi mirëqenies së tij fizike dhe morale.

