Institute
for Democracy
and Mediation

Hanns
Seidel
Stiftung

Balancimi i sigurisë kombëtare dhe të drejtës për privatësi: Implikimet e programeve të mbikëqyrjes shtetërore

Iris Shehaj

Hyrje

Zhvillimet teknologjike kanë revolucionarizuar mënyrën se si ne jetojmë, punojmë dhe komunikojmë. Megjithatë, këto përparime kanë sjellë gjithashtu sfida dhe rreziqe të reja, veçanërisht në fushën e sigurisë kibernetike. Në epokën digjitale, informacioni ynë personal po mblidhet, ruhet dhe analizohet vazhdimisht nga subjekte të ndryshme, duke përfshirë kompanitë private dhe agjencitë qeveritare të sigurisë. Programet e mbikëqyrjes (përgjimit/survejimit) shtetërore janë krijuar me synimin për të mbrojtur vendin nga kërcënimet e mundshme. Megjithatë, këto programe ngrenë shqetësime etike dhe ligjore në lidhje me masën në të cilën privatësia individuale duhet të cënohet në funksion të mbrojtjes së sigurisë kombëtare.

Për më tepër, përparimet në teknologji ngrenë shqetësime të mëtejshme për mundësinë e keqpërdorimit ose abuzimin e mundshëm të kompetencave të mbikëqyrjes shtetërore. Zbatimi i mekanizmave të mbrojtjes, transparencës dhe llogaridhënies mund të garantojë që kjo mbikëqyrje të kryhet brenda kufijve ligjorë, pa shkelur të drejtën e qytetarëve për jetë private.

Ndërveprimi midis sigurisë kibernetike, privatësisë dhe mbikëqyrjes shtetërore është i ndërlikuar dhe shpesh i diskutueshëm. Nga njëra anë, masat e sigurisë kibernetike janë thelbësore për mbrojtjen e privatësisë dhe parandalimin e aksesit të paautorizuar në të dhënat personale. Nga ana tjetër, këto masa mund të përbëjnë kërcënim potencial për privatësinë individuale, nëse nuk respektojnë standardet e të drejtave të njeriut.

Institute
for Democracy
and Mediation

Hanns
Seidel
Stiftung

Konteksi i përgjithshëm

Siguria kibernetike është një koncept që përfshin reduktimin e rrezikut të sulmeve me qëllim të keq ndaj softuerëve, kompjuterëve dhe rrjeteve. Kjo përfshin mjetet, burimet, proceset dhe strukturat e përdorura, për të zbuluar depërtimet, ndalimin e viruseve, bllokimin e aksesit me qëllim të keq, zbatimin e vërtetimit, aktivizimin e komunikimeve të koduara.[1]

Mbikëqyrja, në anglisht surveillance, vjen nga folja franceze surveiller. Ajo lidhet me termin latin vigilare me aludimin se diçka e paqartë, e keqe ose kërcënuese fshihet përtej kullës së vrojtimit dhe mureve të qytetit. Megjithatë kërcënimi mund të shmanget me sukses nga vigjilentët. Në shoqërinë bashkëkohore termi ka një kuptim shumë më të gjerë,[2] sidomos duke përfshirë dimensionin digjital. Përkrahësit e mbikëqyrjes shtetërore argumentojnë se këto programe janë të nevojshme për të zbuluar dhe parandaluar aktet e terrorizmit, krimet kibernetike dhe forma të tjera të kërcënimeve kombëtare, për të mbrojtur qytetarët dhe për të ruajtur rendin publik.

Privatësia, nga ana tjetër, i referohet të drejtës themelore të individëve për t'i mbajtur informacionet, komunikimet dhe aktivitetet e tyre personale, konfidenciale dhe pa ndërhyrje. Teoricienët e hershëm të privatësisë e konceptuan privatësinë në aspektin e kontrollit. Altman për shembull, e përkufizoi atë si "kontroll selektiv i aksesit te vetja ose te grupi i dikujt".[3] Gjithashtu e drejta për privatësi siguron që individët të kenë kontroll mbi të dhënat e tyre personale dhe të merret pëlqimi i tyre për mënyrën sesi ato mblidhen, përdoren dhe shpërndahen.

---

[1] Edward Amoroso, "Cyber Security", New Jersey: Silicon Press, United States of America, 2006.
[2] B. Roessler and D. Mokrosinska, "The Social Dimensions of Privacy". Gary T. Marx, "Coming to Terms: The Kaleidoscope of Privacy and Surveillance", Cambridge University Press, 2015.
[3] Jennifer Jiyoung Suh and Miriam J. Metzger, "Privacy Beyond the Individual Level", Kapitulli 6, "Modern Socio-Technical Perspectives on Privacy", Springer, f. 91, 2022.

Ky artikull trajton marrëdhënien komplekse midis sigurisë kibernetike, të drejtës për privatësi dhe mbikëqyrjes shtetërore në kontekstin e një shoqërie gjithnjë e më digjitale. Artikulli adreson disa nga sfidat dhe shqetësimet që janë shfaqur në këto fusha, duke theksuar nevojën për një qasje të ekuilibruar që mbron sigurinë dhe privatësinë, për të vijuar me një analizë më specifike sesi ky fenomen është zhvilluar në Shqipëri.

Si garantohet mbrojtja e privatësisë?

Qëllimet legjitime për të cilat kryhet mbikëqyrja shtetërore, kryesisht përfshijnë: (i) sigurinë kombëtare; (ii) parandalimin e krimit dhe (iii) sigurinë publike.

E drejta për privatësi në një shoqëri demokratike është me rëndësi kyçe edhe për ushtrimin e të drejtave të tjera me natyrë civile e politike. Duke u garantuar lirinë nga mbikëqyrja (e paligjshme) e shtetit, qytetarët janë të lirë nga presionet dhe ndikimet e paligjshme, janë të lirë të kenë mendimet dhe pikëpamjet e tyre, të mbrohen profilizimi dhe katalogimi i bazuar në tipare të ndryshme të karakterit, janë të lirë për të protestuar dhe për të votuar.[4]

Disa mekanizma për mbrojtjen e të drejtës për privatësi nga mbikëqyrja e palegjitimuar shtetërore përfshijnë:

- Mbrojtja kushtetuese: Shumë vende kanë dispozita kushtetuese që mbrojnë në mënyrë eksplicite të drejtën e individëve për privatësi.
- Legjislacioni: Shtetet miratojnë ligje që rregullojnë në mënyrë specifike aktivitetet e mbikëqyrjes, duke vendosur kufizime se si, kur dhe nga kush mund të kryhet mbikëqyrja. Këto ligje përcaktojnë fushëveprimin e kompetencave të mbikëqyrjes, vendosin kufizime në mbledhjen dhe ruajtjen e të dhënave si dhe vendosin procedura për marrjen e autorizimit të gjykatës.
- Kontrolli i pavarur: Kontrolli gjyqësor dhe ai i institucioneve të pavarura mbi qeverinë, agjencitë e sigurisë dhe ato ligjzbatuese, ndihmon në parandalimin e abuzimeve me kompetencat e mbikëqyrjes. Kontrolli i pavarur synon gjithashtu të sigurojë

[4] Tajdar Jawaid, “Privacy vs National Security”, International Journal of Computer Trends and Technology (IJCTT) – Volume 68 Issue 7, f.2, 2020.

llogaridhënie për veprimet e agjencive shtetërore. Konkretisht, gjyqtarët vlerësojnë dhe autorizojnë kërkesat për mbikëqyrje/përgjim, duke siguruar që ato plotësojnë kërkesat ligjore dhe bazohen në dyshime të arsyeshme. Institucionet e pavarura si Komisioneri për Mbrojtjen e të Dhënave Personale, Avokati i Popullit, sigurojnë mbajtjen e qeverisë përgjegjëse për shkeljet e të drejtave të njeriut në mandatin e tyre.

- Marrëveshjet ndërkombëtare për të drejtat e njeriut: Këto marrëveshje përfaqësojnë angazhime të shteteve në nivel ndërkombëtar për mbrojtjen e të drejtave të njeriut, duke përfshirë të drejtën për privatësi[5], si dhe krijojnë mekanizma për t'i mbajtur qeveritë përgjegjëse për shkeljet që kryejnë.
- Masat teknologjike: Enkriptimi, mjetet e anonimitetit dhe teknologjitë e tjera që përmirësojnë privatësinë ndihmojnë në mbrojtjen e privatësisë së individëve duke mbrojtur komunikimet dhe të dhënat nga mbikëqyrja jolegjitime.
- Transparenca: Transparenca në programet e mbikëqyrjes shtetërore lejon që publiku të jetë i informuar për qëllimin, natyrën, shtrirjen dhe funksionimin e programeve të mbikëqyrjes.

Në realitet, mbikëqyrja shtetërore, veçanërisht programet e mbikëqyrjes masive, mbledhin sasi të mëdha të dhënash personale për individët pa pëlqimin e tyre, me të cilat mund të abuzohet ose mund të keqpërdoren lehtësisht. Kjo ndërhyrje e padrejtë në privatësinë e individit shkel parimin e pëlqimit të informuar dhe minon besimin midis qytetarëve dhe qeverisë së tyre.

E drejta e privatësisë dhe siguria kibernetike në Shqipëri

[5] Thelbi i parimit të privatësisë mund të gjendet në nenin 12 të Deklaratës Universale të të Drejtave të Njeriut, ndërsa të drejtës për privatësi i është dhënë mbrojtje formale ligjore nga Neni 17 i Paktit Ndërkombëtar për të Drejtat Civile dhe Politike dhe neni 8 të Konvetës Evropiane për të Drejtat e Njeriut. Lidhur me mbrojtjen e të dhënave, Komenti i Përgjithshëm Nr. 16 mbi Nenin 17 të Paktit Ndërkombëtar për të Drejtat Civile dhe Politike deklaron që mbledhja dhe ruajtja e informacionit personal duhet rregulluar, pavarësisht nëse mbledhja dhe ruajtja bëhet nga organe publike ose private. Komenti i përgjithshëm pohon gjithashtu se individët kanë të drejtë të dinë se çfarë informacioni ruhet për ta, për çfarë qëllimesh, dhe kush e ruan atë. Ndërsa për herë të parë mbrojtja e të dhënave personale ishte objekt i një marrëveshje ndërkombëtare në Konventën e Strasburgut të datës 28.01.1981 "Për mbrojtjen e individëve në lidhje me përpunimin automatik të të dhënave personale".

E drejta për privatësi dhe mbrojtjen e të dhënave personale në Republikën e Shqipërisë është e garantuar në nenin 35 (1) të Kushtetutës, ku parashikohet se askush nuk mund të detyrohet, përveçse kur e kërkon ligji, të bëjë publike të dhëna që lidhen me personin e tij dhe në nenin 35 (2) ku parashikohet elementi i dhënies së pëlqimit për mbledhjen, përdorimin dhe bërjen publike të të dhënave. Po ashtu, në nenin 36 të Kushtetutës është parashikuar liria dhe fshehtësia e korrespondencës.

Të dhënat personale, sipas ligjit Nr. 9887, datë 10.03.2008 "Për mbrojtjen e të dhënave personale" janë çdo informacion në lidhje me një person fizik, të identifikuar ose të identifikueshëm, direkt ose indirekt, në veçanti duke iu referuar një numri identifikimi ose një a më shumë faktorëve të veçantë për identitetin e tij fizik, fiziologjik, mendor, ekonomik, kulturor apo social.

Është e rëndësishme të theksohet që ndër vite qytetarët shqiptarë janë përballur me shkelje të të drejtës së privatësisë. Ndërhyrje në të drejtën e privatësisë janë bërë edhe në emër të sigurisë kombëtare. Disa prej tyre kanë qënë të natyrës rregullatore dhe ligjore, për shembull: Vendimi nr. 354 datë 04.06.2014 i Këshillit të Ministrave "Për ngritjen e bazës së të dhënave IMEI për regjistrimin e numrave IMEI të aparateve celulare, që përdoren në rrjetet e shërbimeve të komunikimeve të lëvizshme"; dhe neni 131 i ligjit nr. 108/2014 "Për Policinë e Shtetit" për lejimin e përgjimeve nga Policia e Shtetit (edhe) pa autorizim. Të dy këto akte janë shfuqizuar si të papajtueshëm me Kushtetutën.[6]

Më tej, gjatë viteve të fundit, Shqipëria është përballur me rrjedhje të shumta të të dhënave personale të qytetarëve dhe me sulme kibernetike ndaj institucioneve shtetërore. Këto kanë ngritur pyetje të rëndësishme për gatishmërinë dhe kapacitetet e qeverisë shqiptare në administrimin e të dhënave dhe mirëqeverisjen e sektorit të sigurisë kibernetike në zbatim të respektimit të të drejtave të njeriut.

Në prill të vitit 2021, pak javë para zgjedhjeve u publikuan të dhënat personale të 910 mijë zgjedhësve të Tiranës. Të dhënat u shpërndanë në mënyrë elektronike, kryesisht

[6] Shih vendimet e Gjykatës Kushtetuese: Vendimi nr. 57 datë 05.12.2014 dhe Vendimi nr. 30 datë 05.07.2021.

përmes mediave online dhe përmbanin informacione sensitive për qytetarët, përfshirë të dhëna si numri personal i identifikimit, vendi i punës, adresa, numri i telefonit si dhe të dhëna për preferencat apo sjelljet e tyre politike.[7] [8] Një shkelje tjetër e të dhënave personale që ndodhi gjatë vitit 2021 ishte dhe publikimi i pagave të punonjësve të sektorit publik dhe privat. Bazat e të dhënave përmbanin fusha për numrin personal, emrin, mbiemrin, kompaninë, pagën bruto, profesionin. Po ashtu, në 2021 rrodhi një databazë me të dhënat personale të mbi 530 mijë qytetarëve pronarë automjetesh. Në fakt, rrjedhjet e të dhënave të shtetasve shqiptarë datojnë që në vitin 2008, kur baza e të dhënave të gjendjes civile u përhap në mënyrë të paligjshme dhe dispononte emrin, mbiemrin, emrin e babait, emrin e nënës, datën e lindjes, vendin e lindjes, seksin, gjendjen civile.[9]

Çështje shumë të diskutuara kanë qenë edhe sulmet kibernetike ndaj sistemeve shtetërore shqiptare të cilët janë shoqëruar edhe me rrjedhjen e dokumenteve shtetërorë, përveç të dhënave personale. Më datë 09.07.2022, Prokuroria e Rrethit Gjyqësor Tiranë, ka regjistruar procedimin penal për veprat penale: përgjimi i paligjshëm i të dhënave kompjuterike, ndërhyrja në të dhënat kompjuterike, ndërhyrja në sistemet kompjuterike dhe keqpërdorimi i pajisjeve, për sulmin kibernetik ndaj institucionit shtetëror të Agjencisë Kombëtare të Shoqërisë së Informacionit (AKSHI). Po kështu, më datë 09.09.2022 është kryer një tjetër sulm kibernetik në pajisjet dhe sistemet që administrohen dhe menaxhohen nga Ministria e Brendshme në Shqipëri. Këto sulme kibernetike nuk përfshijnë vetëm cënimin e të drejtave për privatësi të qytetarëve, por dhe cënimin e sigurisë kombëtare realizuar nëpërmjet mjeteve teknologjike të hakerimit.

Ajo që u vërejt e domosdoshme pas këtyre sulmeve kibernetike ishte miratimi i një kuadri të ri ligjor për të garantuar sigurinë e të dhënave personale të qytetarëve, por dhe

[7] Orkidea Xhaferaj, Blerjana Bino, Erjon Curraj, "Working Paper: Mapping personal data violations in Albania: A short retrospective on massive breaches in the country", SCiDEV, f.13, 2022, Tiranë
[8] Megi Reçi, Sara Kelmendi, "Tejkalimi i hendekut midis sigurisë kibernetike dhe të drejtave të njeriut" , Instituti për Demokraci dhe Ndërmjetësim, f.14, 2022, Tiranë
[9] Orkidea Xhaferaj, Blerjana Bino, Erjon Curraj, "Working Paper: Mapping personal data violations in Albania: A short retrospective on massive breaches in the country", SCiDEV, f.13, 2022, Tiranë

sigurinë kombëtare dhe kibernetike. Prandaj, për këtë arsye u bënë ndërhyrje në kuadrin ekzistues ligjor; në datën 15.06.2022 u publikua për konsultim publik projektligji "Për mbrojtjen e të dhënave personale" me disa ndryshime; në datën 26.04.2023 u publikua për konsultim publik projekligji "Për Sigurinë Kibernetike"[10]. Ndër të tjera, ky i fundit parashikon ndërhyrje të rëndësishme në kuadrin institucional përkatës për mbrojtjen e sigurisë kibernetike.[11] Ndërsa ndërhyrjet në Ligjin "Për mbrojtjen e të dhënave personale" synojnë harmonizimin me "Rregulloren e Përgjithshme të Bashkimit Evropian për Mbrojtjen e të Dhënave Personale".[12] Një masë tjetër që u ndërmor është dhe miratimi i ligjit nr.43/2023 "Për qeverisjen elektronike" ku është parashikuar dhe detyrimi për mbrojtjen e të dhënave personale.

Përfundime

Si përfundim, përveç masave të ndërmarra për përmirësimin e kuadrit ligjor, në mënyrë që të arrihet një balancë e drejtë midis sigurisë kombëtare dhe të drejtës për privatësi, shteti shqiptar duhet të garantojë kontroll të pavarur mbi shkeljet, ndërmarrjen e masave teknike të nevojshme dhe transparencë. Për të arritur këtë, kërkohet reflektim mbi mësimet e nxjerra nga ngjarjet e të kaluarës së afërt dhe problematikat e të drejtave të njeriut që janë ekspozuar. Cënimet e të dhënave personale dhe sigurisë kibernetike në Shqipëri, dëshmojnë sa i rëndësishëm është trajtimi i sigurisë kibernetike në mënyrë të ndërlidhur me të drejtat e njeriut.

---

[10] Shih Regjistrin Elektronik për Njoftimet dhe Konsultimet Publike: https://konsultimipublik.gov.al/Konsultime/Detaje/626

[11] Aktualisht, kuadri institucional përgjegjës për këtë fushë përfshin: Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), Policinë e Shtetit, Agjencinë Kombëtare të Shoqërisë së Informacionit (AKSHI), Autoritetin e Komunikimeve Elektronike dhe Postare (AKEP).

[12] Shih Regjistrin Elektronik për Njoftimet dhe Konsultimet Publike: https://konsultimipublik.gov.al/Konsultime/Detaje/472