



Viti i XVI-të i Botimit, Nr.2

Dhjetor 2024

FENOMENI I DHUNËS KIBERTINIKE DHE PROBLEMATIKAT AKTUALE TË MBROJTJES JURIDIKO PENALE NDAJ SAJ

Ylli Pjetërnikaj*, Enisa Shahini**

**Prosecutor at the Prosecution Office of First Instance Court of General Jurisdiction - Tirana*

***Judge at First Instance Administrative Court - Tirana*

Përmbledhje

Dhuna kibernetike duke qenë një fenomen relativisht i ri, i cili përfshin një shumëllojshmëri të gjerë krimesh, si term është ende i vështirë për t'u përcaktuar me saktësi. Ajo shpesh keqkuptohet dhe nuk merret seriozisht sa duhet. Megjithatë, mund të fillojë në internet, por shpesh përfundon jashtë realitetit kibernetik me pasoja shkatërruese për viktimat dhe familjet e tyre. Kërcënimet për dhunë, përndjekje, nxitje për vetëvrasje, tërheqje të fëmijëve për qëllime seksuale, të gjitha mund të rezultojnë në vetëlëndimin e viktimës, ose në sulmin fizik nga autori fillestar. Është e rëndësishme të veprohet për të parandaluar shfaqjen e dhunës kibernetike dhe për të mbrojtur e sjellë drejtësi për viktimat.

Shumica e vendeve po përpiqen të njohin aspektet e ndryshme të problemit dhe t'i adresojnë ato në ligjin e tyre të brendshëm. Disa prej tyre kanë ligje që trajtojnë në mënyrë specifike forma të veçanta të dhunës kibernetike. Megjithëse dhuna kibernetike ekziston prej disa vitesh, format e saj specifike duket se kanë filluar të identifikohen dhe kuptohen vetëm kohët e fundit.

Disa lloje të dhunës kibernetike trajtohen plotësisht, ose pjesërisht në marrëveshjet ndërkombëtare, por shumë prej tyre mbeten përsëri të pa adresuara. Prandaj Këshilli i Evropës po punon në të gjithë sektorët e tij (për shembull, përmes mekanizmave që lidhen me Konventën e Budapestit, Konventën e Stambollit dhe Konventën e Lanzarotes) për të siguruar që të drejtat e njeriut të respektohen edhe në hapësirën kibernetike, për të gjithë. Është e rëndësishme të theksojmë se shumë forma të dhunës kibernetike janë tashmë të adresuara në ligjin vendas ose ndërkombëtar nga dispozitat e «botës fizike» dhe hetimet penale nuk duhet të presin vetëm legjislacionin e ri. Kështu, kur kompjuterët përdoren për të shkakuar ose lehtësuar dhunën nëpërmjet transmetimit të mesazheve që shkaktojnë dëme psikologjike, ose nëpërmjet reklamave për vrasje, përdhunim, rrëmbim ose trafikim të qenieve njerëzore, raste të tilla mund të ndiqen penalisht (në varësi të fakteve të tyre) si sulm, shkelje e privatësisë, kanosje, zhvatje, pornografi, ose vrasje, përndjekja, dhuna në familje, etj. Në këtë punim do të fokusohemi tek shfaqja e fenomenit të dhunës kibernetike në Shqipëri, adresimi ligjor i saj, duke identifikuar problematikat përkatesë, dhe nevojat për ndërhyrje.

Fjalë çelës: kibernetike, dhuna, krim, ligji penal, konventa

THE PHENOMENON OF CYBER VIOLENCE AND THE CURRENT PROBLEMS OF CRIMINAL LEGAL PROTECTION AGAINST IT

Abstract

Cyber violence, being a relatively new phenomenon and which includes a wide variety of crimes, as a term in itself is still difficult to be precisely defined. It is often misunderstood and not taken seriously enough. However, it may start online through internet, but often ends up outside cyber reality with devastating consequences for the victims and their families. Threats of violence, stalking, incitement to suicide, attraction of children for sexual purposes, etc. can all result in the victim's self-harm, or physical assault by the original perpetrator. It is important to act in order to prevent cyber violence from occurring, as well as to protect the victims and bring the perpetrators before justice.

Most countries are trying to recognize and acknowledge the different aspects of this phenomenon, and address them in their domestic laws. Some of them have laws that specifically address particular forms of cyber violence. Although cyberbullying has existed for several years, its specific forms seem to have only recently begun to be identified and understood.

Some types of cyber violence are fully or partially addressed in international agreements, but many of them still remain unaddressed. The Council of Europe is therefore working in all its sectors (for example, through mechanisms related to the Budapest Convention, the Istanbul Convention and the Lanzarote Convention) to ensure that human rights are respected for all, even in cyberspace. It is important to note that many forms of cyber-violence are already addressed in domestic or international laws by "physical world" provisions, and criminal investigations should not wait for new legislation. Thus, when computers are used to cause or facilitate violence by transmitting messages that cause psychological harm, or by advertising murder, rape, kidnapping or human trafficking, such cases may be penally prosecuted (depending on the facts) under the provisions of assault, invasion of privacy, threats, extortion, pornography, or murder, stalking, domestic violence, etc.

In this paper we will focus on the appearance of the phenomenon of cyber violence in Albania, the legal addressing of this phenomenon through the identification of its relevant problematics, as well as the need for intervention.

Keywords: *Cyber, violence, crime, criminal law, convention*

1. Përpjekja për të definuar fenomenin e dhunës kibernetike

Aktet e dhunës ndaj individëve të kryera me anë ose të ndihmuara nga teknologjitë e informacionit dhe komunikimit, e identifikuar me termin "*dhuna kibernetike*" janë bërë shqetësimi kryesor për shoqëritë dhe individët në të gjitha vendet e botës. Dhuna kibernetike duke qenë një fenomen relativisht i ri, i cili përfshin shumëllojshmëri të gjerë krimesh, posibilitet për gjërësi të dukurive të saj, diversitet i kategorive dhe nën-kategorive, koncepti për të është ende i vështirë për t'u përcaktuar me saktësi. Grupi i Punës i T-CY¹ për bullizmin kibernetik dhe format e tjera të dhunës, në studimin

1 Komiteti i Konventës për Krimet Kibernetike (T-CY) përfaqëson shtetet palë në Konventën e Budapestit (Këshillit të Europës) për krimin kibernetik. Bazuar në nenin 46 të Konventës, konsultimi i Komitetit synon të lehtësojë përdorimin dhe zbatimin efektiv të Konventës, shkëmbimin e informacionit dhe shqyrtimin e çdo amendamenti të ardhshëm. T-CY 16 (Strasburg, Nëntor 2016), vendosi krijimin e një Grupi Pune T-CY për bullizmin kibernetik dhe format e tjera të dhunës në internet,

e tij “Hartëzimi mbi Dhunën Kibernetike”², arriti konsensus për përdorimin e “*dhunës kibernetike*” si termin më konciz, duke e përcaktuar³ si: “*Përdorimi i sistemeve kompjuterike për të shkaktuar, lehtësuar ose kërcënuar dhunën kundër individëve, që rezulton (ose ka të ngjarë të rezultojë në) dëm ose vuajtje fizike, seksuale, psikologjike ose ekonomike dhe mund të përfshijë shfrytëzimin e rrethave, karakteristikave ose dobësive të individit..*”⁴

Dhënia e një definimi për të paraqet rëndësi të madhë për fokusimin dhe adresimin e saj. Përparësitë e përcaktimit dhe klasifikimit të dhunës kibernetike përfshijnë lehtësimin e njohjes dhe emërtimit të sjelljeve kur ato ndodhin; lejimin e artikulimit të strategjive të rezistencës dhe veprimeve kundërvepruese që janë përshtatur me kërkesat e secilit; dallimin e dhunës kibernetike nga forma të tjera, më pak serioze të sjelljes së “bezdisshme” në internet; zbulimin e marrëdhënieve themelore midis dhunës kibernetike dhe fenomeneve të tjera, të tilla si pornografia, të cilat ndryshe mund të mos zbulohen, duke na ndihmuar të vendosim dhunën kibernetike brenda një perspektive më të gjerë.⁵

Përveç përpjekjeve të tilla institucionale, si ajo e sipërpërmendur, në doktrinë autorë të ndryshëm kanë dhënë definime për termin “*dhuna kibernetike*”. Kështu disa prej tyre e përkufizojnë atë si sjellje në internet, që përbën ose çon në sulm kundër mirëqenies (fizike, psikologjike, emocionale) të një individi ose grupi.⁶ Sipas këtyre studiuësve ajo që dallon dhunën kibernetike nga format tradicionale veçanërisht kundër grave dhe fëmijëve – bazuar në nenin 1.1.j të Rregullores së Procedurës T-CY, si dhetë ngarkojë atë të studiojë temën në formën e një ushtrimi hartografik, duke përfshirë qasjet krahasuese ndaj legjislacionit si dhe dokumentimin e praktikave të mira në funksion të paraqitjes së rezultateve të ndërmjetme në Plenaren e 17-të dhe një raport përfundimtar në Plenarin e 18-të të T-CY. Më pas Plenari i 18-të në nëntor 2017 vendosi të zgjasë mandatin e Grupit të Punës deri më 31 korrik 2018 dhe t'i kërkojë Grupit të paraqesë një draft përfundimtar të studimit të hartës në T-CY 19 (korrik 2018), si dhe të lehtësojë një seminar mbi këtë temë në Konferencën e Oktapodit në korrik 2018.

2 Shih: Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children, “Mapping study on cyberviolence” with recommendations adopted by the T-CY on 9 July 2018, fq 5.

3 Ky përkufizim pune është një përshtatje e kontekstit “kibernetik” të përkufizimit të dhunës ndaj grave sipas nenit 3 të Konventës së Stambollit që e përkufizon atë si shkelje të të drejtave të njeriut dhe një formë diskriminimi ndaj grave dhe do të nënkuptojë të gjitha aktet gjinore- dhunë e bazuar në, ose ka të ngjarë të rezultojë në, dëmtime ose vuajtje fizike, seksuale, psikologjike ose ekonomike për gratë, duke përfshirë kërcënimet për akte të tilla, detyrimin ose privimin arbitrar të lirisë, qoftë në jetën publike ose private.

Në mënyrë të ngjashme, neni 1 i Konventës Ndër-Amerikane për parandalimin, ndëshkimin dhe çrrënjosjen e dhunës ndaj grave (Konventa Belém do Para) e përcakton dhunën ndaj grave si: çdo veprim ose sjellje, bazuar në gjini, që shkakton vdekje ose dëmtime ose vuajtje fizike, seksuale ose psikologjike për gratë, qoftë në sferën publike ose private.

Një përkufizim gjithëpërfshirës i dhunës ndaj grave është dhënë gjithashtu nga Kombet e Bashkuara: “Çdo akt i dhunës me bazë gjinore që rezulton ose ka të ngjarë të rezultojë në dëmtime ose vuajtje fizike, seksuale ose psikologjike ndaj grave, duke përfshirë kërcënimet për akte të tilla, detyrimin ose privimin arbitrar të lirisë, qoftë në jetën publike ose private”. <http://www.un.org/womenwatch/daw/vaw/v-overview.htm>. E përbashkët për të gjitha këto përkufizime është se «dhuna» nuk kufizohet në dëmtim fizik. Anëtarët e Grupit të Punës pranojnë se ky përkufizim pune është mjaft i gjerë dhe duhet të maturohet më tej. Nga ana tjetër, është realitet që çdo krim mund të ketë një element “kibernetik” që mund të ndryshojë natyrën dhe shtrirjen e krimit.

4 Shih: <https://www.coe.int/en/web/cyberviolence>

5 Shih:Herring, Susan C. (2002). “Cyber Violence: Recognizing and Resisting Abuse in Online Environments. *Asian Women* 14 (Summer): 187-212, Indiana University, Bloomington USA.

6 Shih: Herring, Susan C. (2002). “Cyber Violence: Recognizing and Resisting Abuse in Online

të dhunës *offline* është se në të parën, një pjesë e rëndësishme e sjelljes ndodh në internet, megjithëse mund të kalojë më pas në kontekste *offline*. Kështu, dhuna kibernetike mund, por nuk është e nevojshme, të ketë një komponent fizik, dhe shumë nga dëmet e shkaktuara, ashtu si nga dhuna *offline*, janë të natyrës psikologjike dhe/ose emocionale, por nuk do të thotë më pak reale ose shkatërruese. Së fundi, dhuna kibernetike mund të synohet ndaj individëve ose grupeve, të cilët janë objektiva më karakteristik të dhunës kibernetike sesa të dhunës fizike, për shkak të lehtësisë me të cilën një autor i vetëm mund të mbledhë informacione dhe të kontaktojë me një numër të madh njerëzish në internet. Ky është një aspekt tjetër i dhunës në internet që mund të bëjë që ajo të ketë efekte të përhapura.⁷

UN Ëomen konsideron dhunë kibernetike kur një person (ose grup personash) përdor një pajisje të lidhur në internet për të shkaktuar dëmtime seksuale, psikologjike, ekonomike ose të tjera, shpesh duke shfrytëzuar rrethanat, karakteristikat ose dobësitë e targetit të tyre. Dhuna kibernetike shpesh mund të çojë në dëmtim të drejtpërdrejtë fizik. Megjithëse çdokush mund të përjetojë dhunë kibernetike, gratë dhe vajzat janë në rrezik më të madh, veçanërisht ndaj ngacmimeve të rënda dhe abuzimeve seksuale⁸.

Sekretariati i Komunielthit në raportin e tij CVAËG (Cyber Violence Against Women and Girls), e përkufizon dhunën kibernetike si një akt i GBV-së (Gender Based Violence) i kryer drejtpërdrejt ose tërthorazi përmes teknologjive të informacionit dhe komunikimit që rezulton në, ose ka të ngjarë të rezultojë në, dëmtime ose vuajtje fizike, seksuale, psikologjike ose ekonomike për gratë dhe vajzat, duke përfshirë kërcënime të tilla, qofshin ato që ndodhin në jetën publike ose private, apo pengesa për përdorimin e të drejtave dhe lirive të tyre themelore.⁹ CVAËG nuk është i kufizuar, por përfshin shkelje të privatësisë, ndjekje, ngacmim, gjuhë të urrejtjes me bazë gjinore, ndarje personale të përmbajtjes pa pëlqim, abuzimi seksual i bazuar në imazhe, hakimi, vjedhja e identitetit dhe dhuna e drejtpërdrejtë. Dhuna kibernetike është pjesë e vazhdimësisë së VAË (Violence Against Women), sepse ajo nuk ekziston në vakum, përkundrazi, buron dhe mban forma të shumta të dhunës *offline*.¹⁰

Ky përkufizim është gjithëpërfshirës dhe mbetet i gjerë mjaftueshëm për të përfshirë të gjitha format e dhunës kibernetike, duke pranuar vazhdimësinë e VAË midis mjediseve *offline* dhe *online*, si dhe format e ndryshme të dëmtimit të përjetuara nga viktimat. Megjithatë, ai nuk është një përkufizim detyrues dhe nuk përmend në mënyrë eksplicite vajzat, të cilat janë përdorueset të zellshme të teknologjive dixhitale dhe shpesh janë në shënjestër disproporcionale të abuzimit, si një grup i veçantë viktimash.¹¹

Environments. *Asian Women* 14 (Summer): 187-212, Indiana University, Bloomington USA.

7 Po aty.

8 Shih: A Guide for Women and Girls to Prevent and Respond to Cyber violence, 2021 UN Women, fq 4. This guidance note has been produced by UN Women and UNICEF under the joint UN project 'Accelerating Women's Empowerment for Economic Resilience and Renewal: The post-COVID-19 reboot in Armenia', implemented by UNDP, UNIDO, UNICEF and UN Women.

9 "Addressing Online Violence Against Women and Girls in the Commonwealth Europe Region The Role of Bystanders", © Commonwealth Secretariat 2023, fq 8. Ky raport kontribuon në studimin e Commonwealth mbi dhunën në internet kundër grave dhe vajzave (OVAWG) dhe merr në konsideratë prevalencën e dhunës në internet dhe rolin e kalimtarëve, si dhe ligjet, institucionet, politikat dhe praktikën përkatëse për të adresuar problemin në rajonin evropian të Commonwealth, përkatësisht Qipron, Maltën dhe Mbretëria e Bashkuar e Britanisë së Madhe (Anglia, Skocia dhe Uells) dhe Irlanda e Veriut (MB).

10 Shih Scottish Government (2020) Preventing violence against women and girls - what works: evidence summary. Available from <https://www.gov.scot/publications/works-prevent-violence-against-women-girls-summary-evidence/pages/6/>. Accessed 14 March 2024.

11 Shih: EIGE (European Institute for Gender Equality (2022b), 'Cyber violence against women', available at: <https://eige.europa.eu/gender-based-violence/cyber-violence-against-women> (ac-

Gjithashtu të njëjtin qëndrim ka mbajtur edhe Komiteti Këshillimor për Mundësi të Barabarta për Gratë dhe Burrat, i cili e definon dhunën kibernetike ndaj grave si një akt dhune i bazuar në gjini, e ushtruar drejtpërdrejt ose tërthorazi nëpërmjet informacionit dhe teknologjitë e komunikimit që rezultojnë në, ose ka të ngjarë të rezultojë në dëmtim fizik, seksual, psikologjik ose ekonomik ose vuajtjet ndaj grave dhe vajzave, duke përfshirë kërcënimet për akte të tilla qoftë në jetën publike apo private, ose pengesa për përdorimin e të drejtave dhe lirive të tyre themelore. Dhuna kibernetike ndaj grave nuk kufizohet vetëm në, por përfshin shkelje të privatësisë, ndjekje, ngacmim, gjuhë të urrejtjes me bazë gjinore, ndarje të përmbajtjes personale pa pëlqim, abuzim seksual të bazuar në imazhe, hakerim, vjedhje identiteti dhe dhunë të drejtpërdrejtë. Dhuna kibernetike është pjesë e vazhdimësisë së dhunës ndaj grave: ajo nuk ekziston në vakum; përkundrazi, ajo buron dhe mbështet forma të shumta të dhunës jashtë linje.¹²

Dhuna kibernetike, shpesh, keqkuptohet dhe nuk merret aq seriozisht sa duhet. Megjithatë, është e rëndësishme të theksohet se dhuna kibernetike mund të fillojë në internet, por shpesh përfundon jashtë linje me pasoja shkatërruese për viktimat dhe familjet e tyre. Kërcënimet për dhunë, përndjekje, nxitje për vetëvrasje, tërheqje të fëmijëve për qëllime seksuale, të gjitha mund të rezultojnë në vetëlëndimin e viktimës ose në sulmin fizik nga autori fillestar. Është e rëndësishme të veprohet për të parandaluar shfaqjen e dhunës kibernetike dhe për të mbrojtur dhe sjellë drejtësi për viktimat.¹³

Megjithatë, shumica e vendeve po përpiqen të njohin aspektet e ndryshme të problemit dhe t'i trajtojnë ato në ligjin e brendshëm. Disa lloje të dhunës kibernetike trajtohen plotësisht ose pjesërisht në marrëveshjet ndërkombëtare, por shumë mbeten të pa adresuara. Këshilli i Evropës po punon në të gjithë sektorët (për shembull, përmes mekanizmave që lidhen me Konventën e Budapestit, Konventën e Stambollit dhe Konventën e Lanzarotes) për të siguruar që të drejtat e njeriut të respektohen edhe në hapësirën kibernetike, për të gjithë.¹⁴

Informacioni i marrë nga shtetet anetare sugjeron se disa vende kanë ligje që trajtojnë në mënyrë specifike forma të veçanta të dhunës kibernetike. Megjithëse dhuna kibernetike ekziston prej disa vitesh, format e saj specifike duket se kanë filluar të identifikohen dhe kuptohen vetëm kohët e fundit. Shumica e vendeve po luftojnë për të njohur aspektet e ndryshme të problemit dhe për t'i trajtuar ato në ligjin e brendshëm.¹⁵

2. Standartet e GJEDNJ-së mbi dhunën kibernetike

Është e rëndësishme të theksojmë se shumë forma, apo tipologji të dhunës kibernetike janë tashmë të mbuluara në ligjin vendas ose ndërkombëtar nga dispozitat që normojnë “botën fizike” dhe he-

cessed 01 may 2024).

12 Opinion on combatting online violence against women, European Commission Advisory Committee on Equal Opportunities for Women and Men, April 2020.

13 Shih: Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children, “Mapping study on cyberviolence” with recommendations adopted by the T-CY on 9 July 2018, fq 5.

14 Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018.

15 Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, fq 5

timet mund të mos presin, apo stopohen për mungesë legjislacioni. Për shembull, kur kompjuterët përdoren për të shkaktuar ose lehtësuar dhunën nëpërmjet transmetimit të mesazheve, që shkaktajnë dëme psikologjike, ose nëpërmjet reklamave për vrasje, përdhunim, rrëmbim ose trafikim të qenieve njerëzore, raste të tilla mund të ndiqen penalisht (në varësi të fakteve të tyre) si përndjekje, shkelje e privatësisë, kanosje, zhvatje, nxitje përdhunimi ose vrasje, shpërndarja e paligjshme e përmbajtjes (si fotografite), dhuna në familje, etj. Ky është orientim edhe i praktikës së fundit të Gjykatës Europiane për të Drejtat e Njërit, e cila ka identifikuar fenomenin e dhunës kibernetike, ka dhënë një definicion për të, si dhe ka vendosur standartet që duhet të respektohen nga shtetet për adresimin e tij. Sipas saj “cyberviolence” është përdorimi i sistemeve kompjuterike për të shkaktuar, lehtësuar ose kërcënuar dhunën ndaj individëve apo grupeve, duke shkaktuar dëme ose vuajtje fizike, seksuale, psikologjike ose ekonomike. Kjo është arsyeja pse Gjykata Evropiane e të Drejtave të Njërit e ka përfshirë atë midis formave të dhunës në familje.¹⁶ Format e reja të dhunës kibernetike po përhapen, prandaj duhet të përqendrohem në vendimin novator të GJEDNJ, i cili e përfshiu atë mes hipotezave të dhunës në familje.¹⁷

Në veçanti, sipas Gjykatës¹⁸, rastet e dhunës kibernetike si aksesit në të dhënat e ndjeshme të viktimës dhe llogaritë private, gjithashtu, hyjnë në fushën e dhunës në familje. Për rrjedhojë, Shtetet Palë në Konventë duhet të marrin të gjitha masat e nevojshme për të përmbushur detyrimet pozitive të vendosura nga Konventa Evropiane në rastet e dhunës ndaj grave. Në rastet e dhunës në familje, autoritetet kombëtare duhet të refuzojnë një qasje thjesht formaliste dhe të sigurojnë se masat mbrojtëse të marra janë efektive.

Aktet e dhunës kibernetike, ngacmimi kibernetik dhe imitimi me qëllim të keq janë kategorizuar, nga Gjendnj si forma të dhunës kundër grave dhe fëmijëve të afta të minojnë integritetin e tyre fizik dhe psikologjik për shkak të cenueshmërisë së tyre.¹⁹ Gjykata ka vënë në dukje kohët e fundit se “ngacmimi kibernetik njihet aktualisht si një aspekt i dhunës ndaj grave dhe vajzave dhe mund të marrë forma të ndryshme, të tilla si shkeljet kibernetike të jetës private, dhe marrja, shkëmbimi dhe trajtimi i informacionit dhe imazhe, duke përfshirë ato intime”. Në kontekstin e dhunës në familje, partnerët intimë janë shpesh autorë të mundshëm të akteve të përndjekjes ose përgjimit kibernetik.²⁰

Dhuna në internet, ose dhuna kibernetike, është e lidhur ngushtë me dhunën jashtë linje ose “të jetës reale” dhe konsiderohet si një aspekt tjetër i fenomenit kompleks të dhunës në familje.²¹ Shtetet kanë një detyrim pozitiv për të krijuar dhe zbatuar në mënyrë efektive një sistem që ndëshkon të gjitha format e dhunës në familje dhe për të ofruar garanci të mjaftueshme për viktimat.²² Detyrimi pozitiv vlen për të gjitha format e dhunës në familje, qofshin ato jashtë linje apo online.

Gjendnj ka vlerësuar se publikimi i fotografive intime të kërkueses “minoit dinjitetin e saj, duke përcjellë një mesazh poshtërimi dhe mosrespektimi”.²³ Publikimi jo konsensual i fotografive të saj intime,

16 Shih: GJEDNJ çështja e Buturugă v. Romania (application no. 56867/15). ECHR 056 (2020) 10.02.2020.

17 Shih: Edoardo Buffagni “La cyberviolenza è una forma di violenza domestica: come affrontarla” Pubblicato il 10 Feb 2022, [La cyberviolenza è una forma di violenza domestica: come affrontarla - Agenda Digitale](#).

18 Shih: GJEDNJ çështja e Volodinës vs. Rusisë 14/12/2021

19 Shih: KU kundër Finlandës, nr. 2872/02, § 41, GJEDNJ 2008.

20 Shih: GJEDNJ çështja e Buturugă v. Romania (application no. 56867/15). ECHR 056 (2020) 10.02.2020.

21 Shih Buturugă, cituar më lart, §§ 74 dhe 78, dhe paragrafin 20 më lart

22 Shih: çështjet Opuz kundër Turqisë, nr. 33401/02, § 145, ECHR 2009, dhe Bălşan k. Rumania, nr. 49645/09, § 57, 23 maj 2017

23 Shih: GJEDNJ, çështja e Volodinës vs. Rusisë 14/12/2021, cituar më sipër, § 75

krijimi i profileve të rreme në mediat sociale që pretendohej se e imitonin atë, dhe gjurmimi i saj me përdorimin e një pajisjeje GPS ndërhyrë në gëzimin e saj në jetën e saj private, duke e shkaktuar atë të ndiejë ankth, dhe pasiguri. Rrjedhimisht, duhet të përcaktohet nëse autoritetet, pasi kanë marrë dijeni për ndërhyrjen në të drejtat e njëriut sipas nenit 8 të Konventës, kanë përmbushur detyrimet e tyre sipas kësaj dispozite për të marrë masa të mjaftueshme për t'i dhënë fund asaj ndërhyrje dhe për të parandaluar përsëritjen e saj.²⁴

Gjykata së pari do të shqyrtojë nëse shteti i paditur ka krijuar një kuadër ligjor të përshtatshëm që i siguron kërkuarit mbrojtje kundër akteve të dhunës kibernetike.²⁵ Ajo përsërit se, për sa i përket akteve që cenojnë integritetin psikologjik të një individi, detyrimi i një kuadri ligjor adekuat nuk kërkon, gjithmonë, vendosjen e një dispozite të ligjit penal që mbulon veprën specifike. Kuadri ligjor mund të përbëhet, gjithashtu, nga mjete juridike të së drejtës civile të afta për të ofruar mbrojtje të mjaftueshme, mundësisht të kombinuara me mjete juridike procedurale siç është dhënia e një urdhri mbrotjeje.²⁶

Gjykata vlerëson se aktet e dhunës kibernetike që janë “mjaft” serioze për të kërkuar një përgjigje penale nga ana e autoriteteve vendase. Publikimi i fotografive intime të kërkuarës, të llogaritura për të tërhequr vëmendjen e djalit të saj, shokëve të klasës dhe mësueses së tyre, synonte ta poshtëronte dhe degradonte atë. Siç u theksua më lart, gjurmimi i lëvizjeve të saj me anë të një pajisjeje GPS dhe dërgimi i kërcënimeve me vdekje në rrjetet sociale i shkaktuan asaj ankth, shqetësim dhe pasiguri. Gjykata rithekson, gjithashtu, se si interesi publik ashtu edhe interesi i mbrojtjes së viktimave të cenueshme nga veprat penale që cenojnë integritetin e tyre fizik ose psikologjik kërkojnë disponueshmërinë e një mjeti juridik që mundëson identifikimin e autorit dhe sjelljen para drejtësisë.²⁷

Si përmbledhje, Gjykata konstaton se, edhe pse kuadri ekzistues i pajisi autoritetet me mjete ligjore për të ndjekur penalisht aktet e dhunës kibernetike, viktimë e të cilave kërkuarë ishte, mënyra në të cilën ata e trajtuan në të vërtetë çështjen, e veçanërisht një hezitim për të hapur një çështje penale dhe një ritëm i ngadaltë i hetimit që rezultoi në mosndëshkimin e autorit, zbuloi një dështim për të përmbushur detyrimet e tyre pozitive sipas nenit 8 të KEDNJ, duke sjellë rrjedhimisht, shkelje të kësaj dispozite.²⁸

Për më tepër, duke pasur parasysh varësinë nga sistemet kompjuterike, duke përfshirë varësinë psikologjike, fizike dhe ekonomike, disa lloje të krimit kibernetik (qasja e paligjshme në të dhënat personale intime, shkatërrimi i të dhënave, etj.) mund të konsiderohen, gjithashtu, akte të dhunës kibernetike. Ligjet për krimin kibernetik mund të zbatohen veçanërisht kur shkaktohet dhuna si lëndimi ose vdekja, për shembull, nëpërmjet sulmeve të bazuara në kompjuter kundër infrastrukturës kritike, ose pajisjeve mjekësore. Fusha e veprimtimit të të ashtuquajturës “cyberviolence” përfshin një shumësi sjelljesh të dhunshme dhe agresive ndaj të tjerëve dhe, në veçanti, ndaj individëve të pambrojtur.²⁹

Kjo çon në një reflektim të dyfishtë, i cili përqendrohet, nga njëra anë, në llojet e reja të dhunës, apo mënyrat e jashtme të saj, të tilla si përndjekja, ngacmimi kibernetik, bullizimi, apo pornografia hakmarrëse (edhe pse mbeten dyshime të konsiderueshme për sa i përket përshtatshmërisë së kësaj zgjedhjeje të terminologjisë). Nga ana tjetër, mbi zhvillimin dhe konfigurimin e konceptit, domos-

24 Shih: Eremia, cituar më sipër, § 75

25 Shih: *Söderman*, cituar më lart, § 89-91

26 Po aty, §§ 85 dhe 108, me referenca të mëtejshme

27 Shih: KU kundër Finlandës, cituar më lart, § 47, dhe Volodina, cituar më lart, § 100)

28 Shih: **GJEDNJÇështja e Volodinës vs. Ruisë 14/12/2021**

29 Shih: F. Di Tano, I reati informatic e i fenomeni del cyberstalking, del cyberbullismo e del revenge porn, in Th. Casadei, S. Pietropaoli [a cura di], *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters-Kluwer, Cedam giuridica, Milano, 2021, fq. 165-178

doshmërisht për t'u përshtatur me karakteristikat e kontekstit të ri në shqyrtim, të ashtuquajturës “cyberspace”.³⁰ Nga ky këndvështrim, cyberspace është një mjet lehtësues duke iu referuar kryerjes së veprave të paligjshme, për shkak të lehtësisë më të madhe me të cilën lejon të arrijë viktimën, e cila, në ditët e sotme, është pothuajse gjithmonë një subjekt që zakonisht përdor pajisje, duke funksionuar nga lidhja me rrjetin dhe, për këtë arsye, në vendin e zbatimit të sjelljes së paligjshme dhe në të cilën kriminelin pret viktimën e tij.

Cyberspace, siç është strukturuar dhe rregulluar, është një lloj “*kutie e zezë*”, në të cilën grumbullohen sasi të mëdha të dhënash, informacionesh dhe veprimesh, mbi të cilat përdoruesit standardë nuk kanë mundësi reale kontrolli.³¹ Në hapësirën kibernetike, siç vërehet nga Laërence Lessig në esenë e tij të famshme «E drejta e kalit»³², të dhënat mbledhen pa dijeninë e tyre, duke penguar kështu përdoruesin standard të zgjedhë nëse duhet të marrë pjesë apo të pranojë këtë sistem përgjimi.³³ Këto metoda të mbledhjes, përpunimit dhe administrimit të të dhënave çojnë në një përmbysje të fuqisë tradicionale të zotësisë mbi të dhënat e teorizuara nga Lessig, teorikisht, i përket pronarit të të dhënave, të cilat, në fakt, janë në vend të kësaj në zotërim të bartësve të IT-së dhe burimeve kompjuterike.³⁴

3. Tipologjitë kryesore të dhunës kibernetike

Në praktikë, aktet e dhunës kibernetike mund të përfshijnë lloje të ndryshme ngacmimi, përndjekje, shkelje të privatësisë, abuzim seksual dhe shfrytëzim seksual, urrjetje ndaj grupeve ose komuniteteve shoqërore etj. Dhuna kibernetike mund të përfshijë, gjithashtu, kërcënime të drejtpërdrejta ose dhunë fizike, si dhe forma të ndryshme të krimit kibernetik.³⁵ Nuk ka ende një leksik, apo tipologji të qëndrueshme të veprave të konsideruara si dhunë kibernetike dhe shumë nga shembujt e llojeve të dhunës kibernetike janë të ndërlidhura, mbivendosen apo përbëhen nga një kombinim aktesh. Duhet theksuar se jo të gjitha format ose rastet e dhunës kibernetike janë njësoj të rënda, dhe jo të gjitha kërkojnë domosdoshmërisht një zgjidhje ligjore penale, por mund të trajtohen me një qasje të klasifikuar, një kombinim masash parandaluese, edukative, mbrojtëse apo të tjera.³⁶ Në vijim po trajmë disa nga format më përfaqësuese të dhunës kibernetike.

Ngacmimi kibernetik është, ndoshta, forma më e gjerë e dhunës kibernetike dhe përfshin një sjellje

30 Shih: Edoardo Buffagni “La cyberviolenza è una forma di violenza domestica: come affrontarla”Pubblicato il 10 Feb 2022, La cyberviolenza è una forma di violenza domestica: come affrontarla - Agenda Digitale,.

31 Shih Th. Casadei, Corpi, soggetti, reti: una mappa sommaria delle sfide del presente, in Gf. Zanetti – Th. Casadei, Manuale di filosofia del diritto, cit., p. 401)

32 Shih Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. CHI. LEGAL F. 207. The reference is to an argument by Gerhard Casper, who, when he was dean of the University of Chicago Law School, boasted that the law school did not offer a course in “The Law of the Horse.” Id. at 207 (internal quotation marks omitted). The phrase originally comes from Karl Llewellyn, who contrasted the U.C.C. with the “rules for idiosyncratic transactions between amateurs.” Id. at 214.

33 Shih V. Colomba, I diritti nel Cyberspazio. Architetture e modelli di regolamentazione. Con un saggio di Lawrence Lessing, Diabasis, Parma, 2015, pp. 75 e ss., in part. fq. 81

34 Shih: Edoardo Buffagni “La cyberviolenza è una forma di violenza domestica: come affrontarla”Pubblicato il 10 Feb 2022, La cyberviolenza è una forma di violenza domestica: come affrontarla - Agenda Digitale,.

35 Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, fq 6

36 Shih <https://www.coe.int/en/web/cyberviolence>

të vazhdueshme, të përsëritur, e cila synon një person specifik, që është krijuar për të dhe shkakton shqetësime të rënda emocionale, si dhe frikë nga dëmtimi fizik. Ngacmimi kibernetik shpesh realizohet nga një “stuhi abuzimi”.³⁷ Ngacmuesit terrorizojnë viktimat duke kërcënuar me dhunë, postojnë gënjeshtër, apo materiale me përmbajtje shpifëse për t’i shkaktuar viktimës siklet ose më keq midis miqve, familjes ose bashkëpunëtorëve. Ndonjëherë, ngacmuesit manipulojnë motorët e kërkimit për të siguruar lidhjen e gënjeshtërve në kërkimet e emrave të viktimave. Ata pushtojnë privatësinë e viktimave duke postuar informacionet e tyre të ndjeshme, të tilla si imazhe nudo ose numra të identitetit kombëtar.³⁸ Ngacmimi kibernetik, në shumë raste, mund të përshkruhet ose lidhet me “pornografi hakmarrëse”.³⁹

Bullizimi kibernetik është një formë ngacmimi kibernetik, që tentohet të lidhet me viktimë që janë fëmijë, shpesh, të moshës së shkollës së mesme, ndërsa fenomene të tilla si sulmi kibernetik, seksortimi ose «pornografia hakmarrëse» kanë më shumë gjasa të lidhen me të rriturit ose të rinjtë. Kufijtë midis tyre nuk janë të dallueshëm dhe nuk ka marrëveshje të përbashkët se kur të përdoren, cilat terma. Jo të gjitha format e ngacmimit kibernetik përbëjnë domosdoshmërisht një vepër penale. Fenomeni i bullizmit karakterizohet nga veprime të dhunshme dhe frikësuese, si agresioni verbal dhe fizik, format e persekutimit, sjelljet arrogante, të pacipa dhe të përjashtimit social, të kryera me dashje dhe në mënyrë të përsëritur nga një ose shumë persona ndaj një viktime.⁴⁰⁴¹ Për këtë arsye, nga perspektiva e hetimit dhe ndjekjes penale, është thelbësore të bëhet dallimi midis llojeve të ndryshme të bullizmit kibernetik dhe është, gjithashtu, e rëndësishme të bëhet dallimi midis roleve të ndryshme që luajnë individët në një akt të caktuar.

Bullizimi kibernetik përkufizohet në faqen e internetit “Të drejtat e fëmijëve” të Këshillit të Evropës⁴² si përdorimi i teknologjive elektronike për të ngacmuar një person tjetër përmes internetit. Ajo merr formë të ndryshme, që përfshijnë mesazhe të këqija me tekst ose email, thashetheme të dërguara me email ose të postuara në faqet e rrjeteve sociale dhe fotografi, video ose faqe interneti të turpshme

Autorë të ndryshëm kanë dhënë përkufizime të ndryshme të bullizmit kibernetik që mund të konsiderohet gjerësisht si “çdo sjellje e kryer përmes mediave elektronike ose dixhitale nga individë ose

37 Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, fq 7

38 Shih Citron, Danielle K. *Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace*. University of Maryland Francis King Carey School of Law Legal Studies Research Paper, No. 2017-9, 2. See also “the Disturbing Rise of Cyberattacks against Abortion Clinics” in WIRED (10 May 2024)

<https://www.wired.com/story/cyberattacks-against-abortion-clinics/>

39 <https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence>

40 Shih: El Asam, Aiman; Samara, Muthanna. *Cyberbullying and the law: A review of psychological and legal challenge*. Computers in Human Behavior 65 (2016) 127-141.

41 Një shembull i fundit i dhunës kibernetike është sfida “Balena Blu”, e cila është e strukturuar sipas linjave të një videolajë ku pjesëmarrësve u jepen pikë. Fëmijët abonohen në një faqe interneti për t’u kontaktuar nga një “kurator”, i cili do të vendosë 50 detyra që duhet të përmbushen në 50 ditët në vijim. Këto detyra përfshijnë shumë aktivitete, të tilla si shikimi i videove me përmbajtje jashtëzakonisht të dhunshme ose marrja e selfie-ve në situata veçanërisht të rrezikshme (p.sh. në krye të një ndërtese ose afër hekurudhave ose autostradave), por gjithashtu shtrihen deri në vetëlëndim me objekte të mprehta. Detyra e fundit është të kryeni vetëvrasje. Sfida e Balenës Blu duket të jetë e ngjashme me “përkujdesjen” (shih më poshtë); sidoqoftë, “grooming” lidhet në mënyrë tipike në ligjin penal me aktivitetin seksual dhe “Balena Blu” përqendrohet në “prerjen” dhe vetëdëmtimin.

42 <http://www.coe.int/en/web/children/bullying> (link last checked on April 3rd 2024).

grupe që komunikojnë vazhdimisht mesazhe armiqësore ose agresive që synojnë të shkaktojnë dëm ose shqetësim te të tjerët”.⁴³

Viktimat e bullizmit kibernetik përfshijnë gazetarët. Studimi i fundit i Këshillit të Evropës mbi “gazetarët nën presion”⁴⁴ tregoi se gazetarët në më shumë se gjysmën e 47 shteteve anëtare kanë përjetuar ngacmim kibernetik gjatë tre viteve të fundit. Kështu, ngacmimi kibernetik ndikon edhe në lirinë e shprehjes. Nga njëra anë disponueshmëria e disa pajisjeve të afta për të krijuar dhe shkëmbyer imazhe intime kanë sjellë krijimin e matërialeve me përmbajtje pornografike të krijuar nga përdoruesit.⁴⁵ Nga ana tjetër, prodhimi dhe shkëmbimi i imazheve eksplicite seksuale mund të përdoret për aktivitete kriminale si përndjekja në internet, “pornografia hakmarrëse”, biseda me seks,⁴⁶ dhe grooming që përshtaten në kategorinë e përgjithshme të ngacmimeve kibernetike dhe që synojnë kryesisht gratë dhe vajzat.

“*Pornografi hakmarrëse*”⁴⁷ është një term, i cili përqendrohet në portretizimin e qartë seksual të një ose më shumë personave, që shpërndahet pa pëlqimin e subjektit. Fenomeni përfshin kryesisht një partner në një marrëdhënie intime, i cili shpërndan materialin e tillë për të poshtëruar ose frikësuar viktimën. Fenomeni, u shfaq qysh në vitet 1980 (duke qenë një artikull i rregullt në revistën Hustler) dhe u lidh me «pornografinë amatore», përpara se të shndërrohej në video eksplicite seksuale të shpërndara në internet (siç është grumbulluesi amator i pornografisë Xtube në 2008).⁴⁸

43 Shih Tokunaga, Robert S. *Following you home from school: A critical review and synthesis of research on cyberbullying victimization*. Computers in Human Behavior, 26(3), 278. Pwr mw shumw shih Van Leeuwen, J.C. Literature review on the research on cyberbullying definitions. Universiteit Twente. (2012). MOORE, Michael J.; NAKANO Tadashi; ENOMOTO Akihiro; SUDA Tatsuya. *Anonymity and Roles Associated with Aggressive Posts in an Online Forum*. Computers in Human Behavior (2012). JUVONEN, Jaana; GROSS Elisheva F. *Extending the School Grounds?-Bullying Experience in Cyberspace*. Journal of School Health. Vol. 78(9). (2008), 496-505. BESLEY, Bill. Published on <http://www.cyberbullying.ca/> (link last checked 5th of April 2024). SMITH, Peter K.; MAHDAVI Jess; CARVALHO Manuel; FISHER Sonja; RUSSELL Shanette; TIPPETT Neil. *Cyberbullying: its nature and impact in secondary school pupils*. The Journal of Child Psychology and Psychiatry. Vol. 49(4). (2008), 376-385. KOWALSKI, Robin M.; LIMBER, Susan P. *Electronic Bullying Among Middle School Students*. Journal of Adolescent Health 41 (2007) S22-S30. ERDUR-BAKER, Özgür. *Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools*. New Media & Society. Vol. 12(1). (2009), 109-125.

44 Shih Clark, Marilyn/Grech, Anna (2017): Journalists under Pressure. Unwarranted interference, fear and self-censorship in Europe. Council of Europe Publishing. Strasbourg.

45 PAASONEN, Sussanna. *Labors of love: netporn, Web 2.0 and the meanings of amateurism*. New Media & Society 12(8) 1297–1312.

46 Sexchat mund të përkufizohet si “[...] shkëmbim i rastësishëm i pikëpamjeve popullore rreth besimeve, thashethemeve dhe sjelljeve seksuale, të kryera në mënyrë sinkrone ose asinkrone”. Në rastin e bisedës seksuale të bazuar në internet, komunikimi mund të ndodhë në një mjedis të monitoruar ose të pamonitoruar të vendosur nga webmaster. ERNI, John Nguyet. *Sex/Text: Internet Sex Chatting and “Vernacular Masculinity” in Hong Kong*. International Proceedings of Economics Development and Research, Vol. 44, 56-60.

47 <http://luxembourgguidelines.org/english-version/>

48 Në vitin 2010 u hap faja IsAnyoneUp: shpesh jepte informacionin identifikues të subjektit në video. Pronari i faqes, Hunter Moore, u deklarua fajtor për vjedhje identiteti dhe hakerim në vitin 2015. Kevin Bollaert, i cili drejtonte faqen pornografike hakmarrëse UGotPosted, u akuzua në SHBA me 31 akuza, duke përfshirë zhvatjen dhe vjedhjen e identitetit, dhe u dënua në vitin 2015 me 18 vjet burg. Në vitin 2014, një vendim i Ohajos kundër tij dha dëmshpërblim prej 385,000 dollarësh në emër

“*Pornografia hakmarrëse*” është një krim që është njohur nga disa akte ligjore në nivel kombëtar dhe ndërkombëtar, e cila ka përfshirë padi civile dhe vepra penale në vende të ndryshme, edhe pse jo gjithmonë në të njëjtën mënyrë. Përgjithësisht formulimet ligjore kriminalizojnë zbulimin, shpërndarjen, ose promovimin e paligjshëm (domethënë jokonsensuale) të imazheve ose videove intime.

Në SHBA, 35 shtete dhe distrikti i Kolumbisë kanë miratuar ligje për ndjekjen penale të krimeve pornografike hakmarrëse,⁴⁹ ndërsa në Evropë dhe vende të tjera situata është më e fragmentuar ose më pak e rregulluar.⁵⁰ Kanadaja amendoi Kodin e saj Penal (neni 162.1) në mars 2014 për të ndaluar shpërndarjen jo-konsensuale të imazheve intime (ai hyri në fuqi në mars 2015). Një dispozitë shoqëruese (seksioni 162.2, i ndryshuar në 2015) autorizon gjykatën të urdhërojë heqjen e imazheve intime nga interneti, i lejon asaj të urdhërojë konfiskimin e kompjuterit, celularit ose pajisjes tjetër të përdorur për veprën penale; parashikon rimbursimin e viktimave për shpenzimet e bëra në heqjen e imazhit intim nga interneti ose gjetkë; apo të marrë një urdhër për të parandaluar dikë që të shpërndajë imazhe intime. Në Gjermani në maj të vitit 2014, jurisprudenca vendosi që fotografitë intime të partnerëve duhet të fshihen nëse partneri e kërkon atë. Vendimi i Gjykatës së Lartë Rajonale Gjermane të Koblenz-it është dhënë për rastin e një personi i divorcuar, i cili refuzoi të fshinte imazhet erotike të ish-bashkëshortes së tij pas ndarjes së tyre.⁵¹ Në Francë, në vitin 2016, me anë të ligjit nr. 2016-13 të datë 7 tetor 2016 titulluar “Ligji i Republikës dixhitale” u bënë ndryshime në Kodin penal duke kriminal

izuar në mënyrë specifike pornografinë hakmarrëse.⁵²⁵³

Në vitin 2015, Mbretëria e Bashkuar ndryshoi Aktin e Drejtësisë Penale dhe Gjykatave, duke përfshirë në elementet e figurës së vepres penale “Vepra që përfshijnë qëllimin për të shkaktuar shqetësim”, aktin e zbulimit të fotografive dhe videove seksuale intime me qëllim për të shkaktuar shqetësim.⁵⁴

Shumë forma të dhunës kibernetike përfaqësojnë, ose lidhen me shkeljen e privatësisë së viktimave, TIKU-t⁵⁵. Kjo mund të përfshijë ndërhyrje kompjuterike për marrjen, vjedhjen, zbulimin ose manipulimin e të dhënave intime, kërkimin dhe transmetimin e të dhënave personale (“doksing”), ose akte të tilla si “përndjekje kibernetike” ose “shkëputje/pornografi hakmarrëse”.⁵⁶

Cyberstalking⁵⁷ i referohet përndjekjes në një format elektronik. Me anonimitetin, lehtësinë dhe efik-

të një të mituri të paraqitur në foto. Raste të tjera janë akuzuar në Mbretërinë e Bashkuar vitet e fundit.

49 Shih: <https://www.cybercivilrights.org/revenge-porn-laws/>

50 Shih: Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018, fq 9

51 Shih: <https://www.thelocal.de/20140522/court-forces-ex-lovers-to-delete-sexy-photos>

52 Në nenin 67 të këtij ligji është parashikuar se: “Kur veprat e parashikuara në nenet 226-1 dhe 226-2 kanë të bëjnë me fjalë ose imazhe të natyrës seksuale të bëra në një vend publik ose privat, dënimet rriten me dy vjet burgim deri në dy vjet deri në 1000 €. Të njëjtat sanksione zbatohen për faktin, në mungesë të pëlqimit të personit për shpërndarje, për të sjellë në vëmendjen e publikut ose të një pale të tretë çdo regjistrim ose dokument që lidhet me fjalë ose imazhe të një natyre prezente, të marra, me pëlqimin e shprehur ose të supozuar të personit ose të tyre, duke përdorur një nga aktet e parashikuara në neni 226-1.22..”.

53 Shih: https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3271AC-8D94E47247A2CFDC0389186E84.tpdila17v_1?idArticle=JORFARTI000033203291&cidTexte=JORFTEXT000033202746&dateTexte=29990101&categorieLien=id

54 Shih: <http://www.legislation.gov.uk/ukpga/2015/2/section/33>

55 Information and Communications Technology

56 <https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/>

57 Përdorimi i përsëritur i komunikimeve elektronike për të ngacmuar ose frikësuar dikë, për

asitetin e internetit, sulmi kibernetik mund të ndodhë në shumë mënyra. Ndjekësit kibernetikë mund të përdorin informacione personale për viktimën për të kërcënuar ose frikësuar viktimën. Sulmusit kibernetikë mund të dërgojnë, gjithashtu, emaille të padëshiruara, të përsëritura ose mesazhe të menjëhershme që mund të jenë kërcënuese armiqësore në natyrë. Përndjekësit kibernetikë mund të imitojnë viktimat e tyre në internet duke vjedhur informacionin e hyrjes për një llogari emaili, ose faqe në rrjetet sociale, dhe në vijim duke postuar mesazhe në faqet e kolegëve të tjerë”.⁵⁸

“Përndjekja përfshin një model sjelljesh të përsëritura, ndërhyrëse, të tilla si ndjekja, ngacmimi dhe kërcënimi, që shkaktojnë frikë te viktimat”.⁵⁹ Vitet e fundit, ky fenomen ka përfshirë gjithnjë e më shumë përdorimin e teknologjive celulare (të tilla si telefonat inteligjentë) si dhe kompjuterët, laptopë, tableta dhe kamera dixhitale. Studimet tregojnë se partneret meshkuj janë autorët kryesorë të përndjekjes së partnerit intim. Gjithashtu ato tregojnë se gratë kanë më shumë gjasa të përndjehen sesa burrat dhe kanë më shumë gjasa të përjetojnë frikë për shkak të përndjekjes.⁶⁰

Hulumtimet tregojnë se përndjekja kibernetike nga partnerët intimë shpesh ndodh në kontekstin e dhunës në familje dhe është një formë kontrolli shtrëngues.⁶¹ Përndjekja nga partnerët intimë mund të jetë e vazhdueshme dhe e rrezikshme. Studiuesi Woodlock i referohet një sondazhi kombëtar të SHBA-së që “gjeti se rastet që përfshinin partnerë intimë zgjatën mesatarisht 2.2 vjet, krahasuar me 1.1 vjet për ndjekjen nga të tjerët” dhe ka qenë e lidhur me vrasjet, apo tentative për të. TIK-të përdoren jo vetëm për të mbajtur viktimën nën vëzhgim (kamera dixhitale të fshehura, gjurmimi GPS i automjeteve), por përfshijnë ngacmimin dhe kontrollin përmes emailleve të vazhdueshme dhe mesazheve të vazhdueshme SMS (SMS). Sjellja që në kontekste të tjera kryhet në mënyrë konsensuale për kënaqësi, si p.sh. “sexting”, përdoret në mënyrë shtrënguese dhe jo konsensuale për të kontrolluar, ngacmuar ose turpëruar nga partnerët intimë të përfshirë në sulm në internet.⁶²

Sextortion është një term, i cili i referohet aktiviteteve që përfshijnë manipulim ose shtrëngim për shembull duke dërguar email kërcënues.

58 Shih: Marcum, Catherine D.; Higgins, George E.; Ricketts, Melissa L., *Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration*. International Journal of Cyber Criminology, Vol. 8, Issue 1, 48.

59 Shih: Woodlock, Delanie (2016): *The Abuse of Technology in Domestic Violence and Stalking*. Violence Against Women. Volume: 23 issue: 5, page(s): 584-602 <http://journals.sagepub.com/doi/full/10.1177/1077801216646277> (link last checked on March 29, 2017)

60 Shih: Woodlock 2016: 584-585

61 Shih: Woodlock (2016: 585) sqaron se: “Kontrolli shtrëngues është një kuadër teorik që përfshin abuzimin fizik që ndodh në dhunën në familje, por që përfshin gjithashtu taktika që nuk shihen tradicionalisht si forma serioze abuzimi. Këto taktika përfshijnë strategji për të kontrolluar dhe frikësuar, të tilla si izolimi, survejimi, kërcënimet me dhunë, mikromenaxhimi i aktiviteteve të përditshme (p.sh., rregullimi i dushit dhe të ngrënit) dhe turpërimi (Stark 2007). Teoria e kontrollit shtrëngues përfshin gjithashtu efektet mbi viktimat e këtyre taktikave. Stark (2012) beson se këto efekte kanë më shumë të përbashkëta me përvojat e pengjeve dhe viktimave të rrëmbimeve sesa të viktimave të sulmeve konvencionale. Stark pranon se megjithëse gratë mund të jenë abuzive në marrëdhëniet intime, burrat janë autorët kryesorë të kontrollit shtrëngues, sepse është një formë dhune e rrënjësuar në pabarazinë sistematike, e cila u jep burrave një privilegj të bazuar në seks. Stark e sheh këtë privilegj të bazuar në seks si thelbin e kontrollit shtrëngues, ku shkelësit meshkuj ‘shfrytëzojnë pabarazitë e vazhdueshme seksuale në ekonomi dhe në mënyrën se si rolet dhe përgjegjësitë janë caktuar në shtëpi dhe komunitet për të vendosur një regjim formal të dominimit/nënshtrimit pas të cilit ata mund të mbrojnë dhe zgjerojnë privilegjin e tyre’(f.206).

62 Shih: Woodlock 2016: 587-588. ICT-facilitated stalking can thus be associated with the phenomenon which the internet and media dubbed “revenge-porn” which often involves public humiliation of the victim.

të kryer aktivitete seksuale për të mirën e agresorit dhe/ose për të krijuar imazhe të qarta seksuale të viktimës dhe krimin tradicional të zhvatjes. Megjithëse krimi mund të përfshijë kërcënimin për të shpërndarë imazhe ose video të tilla pasi ato të jenë krijuar, është po aq e zakonshme që shtrëngimi mund të përfshijë kërcënimin për të lënduar familjen ose miqtë e viktimës nëse aktiviteti seksual nuk ndërmerret, apo regjistrohet ose transmetohet tek agresori. Motivi i agresorit mund të jetë gjithashtu hakmarrja, poshtërimi ose përfitimi monetar. Shpesh kryhet nga distanca përmes rrjeteve kompjuterike dhe mund të përfshijë regjistrimin e imazheve ose transmetimin e drejtpërdrejtë të videos (d.m.th., duke përdorur një kamerë në internet). Autorët janë shpesh partnerë aktualë, ose ish-partner romantikë, ose seksualë.⁶³

Kërcënime të drejtpërdrejta të lidhura me TIK-un ose dhunë aktuale. Dhuna kibernetike gjithashtu përfshin kërcënime të drejtpërdrejta me dhunë ose dhunë fizike të drejtpërdrejtë. Sistemet kompjuterike mund të përdoren në lidhje me vrasjen, rrëmbimin, përdhunimin dhe akte të tjera të dhunës seksuale ose zhvatje. Format e dhunës së drejtpërdrejtë përfshijnë ndërhyrjen në pajisjet mjekësore që shkaktojnë lëndime ose vdekje,⁶⁴ ose sulme kundër infrastrukturës kritike me anë të kompjuterëve.

“Sëatting” është një shembull se si sistemet kompjuterike mund të keqpërdoren për shumë lloje sjelljesh me ndikim të dhunshëm mbi viktimat. Kjo ka të bëjë me përdorimin e telefonave dhe sistemeve kompjuterike për të mashtruar një shërbim urgjence në mënyrë që të dërgojë forcat e rendit në një vend të caktuar bazuar në një raport të rremë. Emri vjen nga akronimi “S.Ë.A.T.” (Armët dhe Taktikat Speciale), të cilat janë njësi të zbatimit të ligjit që kanë trajnime të specializuara dhe mund të përdorin pajisje të stilit ushtarak. Raportet e rreme përfshijnë raportimin e vrasjeve në shtëpinë e dikujt tjetër, kërcënimet me bombë dhe rrëmbimin. «Sëatting» mund të përfshihet në një sërë krimesh, të tilla si kërcënimet me vdekje, komploti për të kryer mashtrime, pengimi i drejtësisë dhe prishja e qetësisë publike. Këto nuk janë thjesht telefonata shakaje, autorët zakonisht përdorin mashtrimin e ID-së së telefonuesit dhe inxhinierinë sociale dhe disa demonstrojnë përdorimin e sofistikuar të sistemeve dhe programeve kompjuterike për ta bërë të duket se telefonatat vijnë nga vende të ndryshme (ndonjëherë në vende të ndryshme nga pika e origjinës së shkelësit).⁶⁵ Sëatting mund të jetë e rrezikshme për viktimat, të cilat, në disa raste janë vrarë nga forcat e rendit, ose që kanë pësuar lëndime fizike.⁶⁶

4. Nevoja për ndërhyrje ligjore

Ndërsa parandalimi është thelbësor dhe duhet t’i jepet përparësi, drejtësia penale është pjesë e reagimit. Duhet të sigurohet një trajnim dhe ngritje më e mirë e ndërgjegjësimit të autoriteteve të drejtësisë penale lidhur me dhunën kibernetike (përfshirë hetimin, ndjekjen penale dhe sanksionimin e saj, ku përbën një vepër penale). Duhet të përdoren mjetet e disponueshme të mbrotjes juridiko penale sipas Konventave të Budapestit e protokollit të parë shtesë, Lanzarote dhe Stambollit të Këshillit të Evropës, por edhe Konventës për Veprimin kundër Trafikimit Njerëzor, nëse Shtetet janë apo jo Palë të këtyre instrumenteve.⁶⁷

63 <https://www.wearethorn.org/sextortion/1880/> (link last checked 4th of April 2024).

64 <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/>

65 Në vitin 2009, phreaker i verbër Matthew Weigman u dënua me 11 vjet burg në Shtetet e Bashkuara për swatting. Në vitin 2014 në British Columbia, Kanada, një adoleshent duke përdorur dorezën «Obnoxious» kreu 40 akte të tentativës ose të suksesshme të goditjes në disa vende. Ai u deklarua fajtor për 23 akuza.

66 <https://www.justice.gov/usao-md/pr/british-and-american-men-indicted-swatting>; <https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1>; <https://www.fbi.gov/contact-us/field-offices/minneapolis/news/press-releases/houston-texas-area-teenager-sentenced->

67 Shih: Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and oth-

Këto standarde ndërkombëtare të Këshillit të Evropës ofrojnë udhëzime dhe mjete të vlefshme për shtetet në trajtimin dhe mbrojtjen ndaj dhunës kibernetike. Legjislacioni ekzistues i vendit tonë, i harmonizuar me konventat e sipërpërmendura mund të jetë në disa rrethana i përshtatshëm për të operacionet kualifikuese të dhunës kibernetike në elementet konkrete të veprave penale, ose mund të cilësohet përsa është e mundur sipas normave të veçantë të kuadrit juridik për krimin kibernetik. Megjithatë dhuna kibernetike në tërësinë e saj mbetet e paadresuar në legjislacionin penal të vendit tonë. Është e rëndësishme që në aspektin e teknikës legjislative të hartohen dispozita penale, që hipotezat e tyre të jenë teknologjikisht neutrale në mënyrë që të sigurohen se ato mund të zbatohen për teknologjitë në zhvillim dhe format e ardhshme të cyberviolence. Suksesi i bashkëpunimit ndërkombëtar për llojet e reja të krimit mund të ndikohet nga niveli i kriminalizimit të cyberviolence në shtete.

Shumica e shteteve kanë legjislacion që kriminalizon sjelljen në lidhje me shfrytëzimin seksual dhe abuzimin e fëmijëve në internet,⁶⁸ apo kriminalizon formave të tjera të dhunës kibernetike si ngacmimi kibernetik, ngacmimi, dhe të tjera që janë zhvillim më i fundit. Disa shtete përfshijnë përgjegjësinë e ofruesve të shërbimeve. Shumica e shteteve duket se zbatojnë ligjin e rregullt penal dhe dispozita të tjera, por asnjëra prej tyre nuk ka një legjislacion të plotë. Për shembull: ⁶⁹ Austria ka penalizuar në nenin 107-c të Kodit Penal titulluar “*Ngacmimin e vazhdueshëm që përfshin sistemet e telekomunikacionit ose kompjuterit*” duke parashikuar se: “(1) Çdo person i cili, duke përdorur një sistem telekomunikacioni ose kompjuterik në një mënyrë që mund të shkaktojë ndërhyrje të paarsyeshme në stilin e jetës së personit tjetër, vazhdimisht për një periudhë më të gjatë kohore 1. shpif tjetrin në një mënyrë që mund të perceptohet nga numër më i madh personash, ose 2. vë në dispozicion fakte ose materiale vizuale të sferës personale të një tjetri për një numër më të madh njerëzish pa pëlqimin e personit tjetër, dënohet me burgim deri në një vit ose me gjobë deri në 720 njësi dënimi. (2) Personi dënohet me burgim deri në tre vjet nëse vepra rezulton me vetëvrasje ose tentativë për vetëvrasje nga viktima nga para. 1.”

Në vitin 2016, Franca miratoi ‘Ligjin e Republikës Dixhitale’, i cili përfshin një sanksion më të ashpër të atyre që shpallen fajtorë për pornografi hakmarrëse. Sipas legjislacionit të ri, autorët përballen me një dënim me dy vjet burg ose një gjobë prej 60 000 €.

Gjermania, si shumë shtete të tjera, përdor dispozita të ligjit penal që nuk janë specifike për mjedisin në internet.⁷⁰ Megjithatë në vitin 2017 u bërë reforma penal në këtë drejtim me anë të miratimit të aktit për përmirësimin e zbatimit të ligjit në rrjetet sociale, i cili është zbatuar për detyrimet e pa-

er forms of online violence, especially against women and children, “Mapping study on cyberviolence” with recommendations adopted by the T-CY on 9 July 2018, fq 10

68 Për shembuj të kriminalizimit shih Këshilli i Evropës/Divizioni për Mbrojtjen e të Dhënave dhe Krimin Kibernetik (2012): Mbrojtja e fëmijëve kundër dhunës seksuale: standardet e ligjit penal të Konventave të Budapestit dhe Lanzarote (Dokument diskutimi), Strasburg, dhjetor 2012.

69 Pwr shwmbuj tw kriminalizimit shih: Council of Europe/Data Protection and Cybercrime Division (2012): Protecting children against sexual violence: the criminal law benchmarks of the Budapest and Lanzarote Conventions (Discussion paper), Strasbourg, December 2012.

70 P.sh. neni 238 i Kodit Penal Gjerman (Stalking), seksioni 240 (Përdorimi i kërcënimeve ose i forcës për të bërë që një person të bëjë, të vuajë. ose hiq një akt), neni 241 (Kanosja për kryerjen e një krimi), neni 176 (Abuzim i fëmijëve), neni 185 (Fyerje), neni 186 (Shpifje), neni 187 (Shpifje me dashje), neni 201 (Shkelje e privatësisë i fjalës së folur) dhe neni 201a (Shkelja e privatësisë intime duke bërë fotografi) të Kodit Penal Gjerman (Strafgesetzbuch) si dhe neni 33 i Ligjit në lidhje me të drejtat e autorit në lidhje me veprat e arteve pamore dhe fotografisë (Kunsturhebergesetz). Seksioni 238 (Përndjekja) përfshin shprehimisht sjelljen me anë të telekomunikacionit (para. 1 nr. 2) ose duke përdorur të dhënat personale të një personi (para. 1 nr. 3). E njëjta gjë vlen edhe për nenin 176 (Abuzimi i fëmijëve) i cili gjithashtu mbulon shprehimisht sjelljen me anë të telekomunikacionit (para. 4 nr. 3 dhe 4).

jtueshmërisë për rrjetet sociale, por nuk po e zgjeron fushën e kriminalizimit.

Italia në maj 2017 miratoi ligjin nr. 71/2017, me titull “Rregullorja për mbrojtjen e të miturve dhe parandalimin dhe trajtimin e bullizmit kibernetik”. Ky ligj fokusohet vetëm në bullizimin kibernetik.⁷¹

Në Mbretërinë e Bashkuar, në prill 2015, u penalizua me një maksimum prej dy vitesh burgim, shpërndarja e fotografive ose videove private seksuale pa pëlqimin e subjektit me qëllim që të shkaktojë shqetësim tek ata që ishin në shënjestër. Në shtator 2016 u njoftua se më shumë se 200 persona ishin ndjekur penalisht që nga hyrja në fuqi e ligjit. SHBA-ja e kriminalizon “përndjekjen kibernetike” në 18 Kodin Amerikan të Seksionit 2261A(2).⁷²

Modeli i tekstit legjislativ për krimin kibernetik (ITU 2012)⁷³, ofron një zgjidhje sesi duhet të jetë hipoteza e kriminalizimit të dhunës kibernetike. Kështu në nenin 18 të këtij teksti është parashikuar figura e vepres penale “Ngacmimi duke shfrytëzuar mjetet e komunikimit elektronik”, me përmbajtje: *“Një person, i cili pa justifikim ose justifikim të ligjshëm ose mbi një justifikim ose justifikim të ligjshëm fillon çdo komunikim elektronik, me qëllim për të detyruar, frikësuar, ngacmuar ose shkaktoar shqetësime të konsiderueshme emocionale te një person, duke përdorur një sistem kompjuterik për të mbështetur sjellja e rëndë, e përsëritur dhe armiqësore, kryen një vepër të dënueshme, në bazë të dënimit, me burgim për një periudhë jo më të gjatë, ose me gjobë që nuk e kalon [shumën], ose të*

71 Neni 1 i ligjit e përkufizon bullizmin kibernetik si: “çfarëdo forme presioni psikologjik, agresioni, ngacmimi, shantazhi, lëndimi, fyerja, denigrimi, shpifja, vjedhja e identitetit, ndryshimi, përvetësimi i paligjshëm, manipulimi, përpunimi i paligjshëm i të dhënave personale të të miturve dhe/ose shpërndarja. bërë përmes mjeteve elektronike, duke përfshirë shpërndarjen e përmbajtjes në internet që përshkruan gjithashtu një ose më shumë përbërës të familjes së të miturit, qëllimi i qëllimshëm dhe mbizotërues i të cilëve është të izolojnë një të mitur ose një grup të miturish duke vënë në fuqi një abuzim serioz, një sulm me qëllim të keq ose një përhapje të gjerë. dhe tallje të organizuar...”.

72 Nw kwttw nen parashikohet se: “Kushdo që...(2) me qëllim për të vrarë, plagosur, ngacmuar, frikësuar ose vendosur nën vëzhgim me qëllim për të vrarë, plagosur, ngacmuar ose frikësuar një person tjetër, përdor postën, çdo shërbim kompjuterik interaktiv ose shërbim të komunikimit elektronik ose sistem të komunikimit elektronik të tregtia ndërshtetërore, ose çdo objekt tjetër i tregtisë ndërshtetërore ose të jashtme për t’u përfshirë në një drejtim që- (A) e vendos atë person në frikë të arsyeshme nga vdekja ose lëndimi i rëndë trupor i një personi të përshkruar në pikën (i), (ii) ose (iii) të paragrafit (1) (A); ose (B) shkakton, përpjekje për të shkaktoar ose në mënyrë të arsyeshme pritët të shkaktojë shqetësim të konsiderueshëm emocional tek një person i përshkruar në pikën (i), (ii) ose (iii) të paragrafit (1) (A), do të dënohet...”. SHBA ka gjithashtu një dispozitë specifike për “zhvatjen që përfshin kompjuterë” (18 Kodi i SHBA-së, Seksioni 1030(a)(7)), i cili përfshin kërcënime për të shkaktoar dëme në një kompjuter ose kërcënime për marrjen e informacionit nga një kompjuter i mbrojtur...”.

73 Shih: Establishment of Harmonized Policies for the ICT Market in the ACP Countries, Cyber-crime/e-Crimes: Model Policy Guidelines & Legislative Texts Harmonization of ICT Policies, Leg-

islation and Regulatory Procedures in the Caribbean. Modeli i tekstit legjislativ –Krimi Kibernetik/Krimet elektronike, nw kuadwr tw Projektit HIPCAR qw është: “Rritja e konkurrencës në Karaibe përmes Harmonizimit të TIK-ut Politikat, Legjislacioni dhe Procedurat Rregullative”. Projekti HIPCAR u lançua nga Unioni Ndërkombëtar i Telekomunikacionit (ITU) dhe Bashkimi Evropian (KE) në dhjetor 2008, në bashkëpunim të ngushtë me Sekretariatit e Komunitetit të Karaibeve (CARICOM) dhe Unionin e Telekomunikacionit të Karaibeve (CTU). Projekti HIPCAR është pjesë e një projekti global ITU-EC-ACP që përfshin gjithashtu Afrikën Sub-Sahariane dhe Paqësorin.

dyja...”. Gjatë viteve të fundit fenomeni i dhunës kibernetike ka njohur zhvillime dhe dimensione të reja. Prandaj edhe kjo zgjidhje e ofruar nuk është plotësisht adekuate. Këto aspekte janë marrë në konsideratë nga hartuesit e draftit të Kodit të ri Penal në Republikën e Shqipërisë. Në këtë draft është parashikuar në mënyrë eksplicitë kriminalizimi i dhunës kibernetike, duke parashikuar në hipetëzën e saj format tipike e shfaqjes së saj.⁷⁴

Rekomandime dhe konkluzione:

- Dhuna kibernetike synon shumë njerëz bazuar në karakteristikat e tyre, ose anëtarësimin në grupe të caktuara. Legjislacioni i botës fizike në vende të ndryshme mbron grupe të ndryshme shoqërore dhe nuk do të ishte e mundur të renditeshin të gjitha bazat mbi të cilat njerëzit synohen ose mbrohen posaçërisht. Megjithatë, disa baza të njohura do të ishin: mosha, shtetësia, ngjyra, përkatësia etnike, gjuha, statusi martesor, origjina kombëtare, sfidat fizike, raca, feja, seksi, orientimi seksual dhe statusi social (veterani ushtarak, oficer policie, refugjat, etj.). Sigurisht që viktimat mund të jenë në shënjestër për më shumë se një arsye.
- Gjykata Evropiane e të Drejtave të Njeriut e mbajtur në K.U. kundër Finlandës,⁷⁵ që shtetet kanë një detyrim pozitiv për të mbrojtur qytetarët nga krimi, duke përfshirë cenimet e jetës private. Prandaj organet e ushtrimit të ndjekjes penale kanë detyrimin të kryejnë hetime dhe ndjekje penale të akteve të dhunës kibernetike. Shtetet duhet ta marrin seriozisht dhunën kibernetike dhe të kujdesen për ndryshimin e ligjeve, përmirësimin e aftësive hetimore.
- Për shkak se dhuna kibernetike mund të lidhet ose të çojë në pasoja fizike, duke përfshirë sulmet fizike, vendet duhet të sigurojnë që ligjet e tyre online dhe offline të jenë në harmoni: kërcënimet elektronike mund të jenë jo më pak të tmerrshme sesa kërcënimet në letër. Për më tepër, ligjet duhet të shkruhen në terma teknologjikisht neutrale, duke qenë koncize dhe të diferencuara në të njëjtën kohë. Me zhvillimin e krimit elektronik, ligjet e hartuara në mënyrë fleksibël do të jenë në gjendje më së miri ta trajtojnë atë.

Referencë:

74 Në nenin 241 të draft kodit titulluar “Ngacmimi duke shfrytëzuar mjetet e komunikimit elektronik”, është parashikuar se: “... 1. Një person, i cili pa të drejtë fillon çdo komunikim elektronik, me qëllim për të detyruar, frikësuar, ngacmuar ose shkaktuar shqetësime të konsiderueshme emocionale te një person tjetër, duke përdorur një sistem kibernetik, kryen keqpërdorim të të dhënave personale, bën që persona të tjerë t’iu kontaktojnë, kërcënon me dëmtim të jetës, integritetit fizik, shëndetit ose lirisë së tij, të një të afërmi të tij ose të një personi tjetër të afërt, shpërndan një imazh të këtij personi, një prej të afërmeve të tyre ose një personi tjetër të afërt me ta ose, e bën atë të aksesueshme për publikun, shpërndan materiale me përmbajtje që e bën personin të neveritshëm ose degradues në opinionin publik, nën pretendimin e autorësisë së personit ose, të bëhet i aksesueshëm për publikun, ose kryen sjellje të tjera të rënda, të përsëritur dhe armiqësore, dënohet me burgim nga një deri në katër vjet.

2. Po kjo vepër kur shkakton vdekjen e viktimës apo dëmtim të rëndë të shëndetit të saj, të një të afërmi të viktimës ose një personi tjetër të afërt me viktimën, e vë viktimën, një të afërm të saj ose një person tjetër të afërt me viktimën në rrezik të vdekjes ose dëmtimit serioz të shëndetit, autori do të përgjigjet për pasojën e ardhur bazuar në dispozitën e veçantë që parashikon atë nëpjesën e posaçmetë këtij Kodi, në varësi të formës së fajit të shfaqur prej tij.

3. Nëse viktimë është i mitur, dënimi i bashkuar penal për veprat e kryera shtohet deri në një të dytën e tij...”.

75 Shih: *Ceshtja K.U. v. Finland* 02.12.2008 (European Court of Human Rights, no. 2872/02).

1. A Guide for Women and Girls to Prevent and Respond to Cyberviolence, 2021 UN Women.
2. Addressing Online Violence Against Women and Girls in the Commonwealth Europe Region The Role of Bystanders”, © Commonwealth Secretariat 2023,
3. Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children, “Mapping study on cyber-violence” with recommendations adopted by the T-CY on 9 July 2018.
4. Konventës Ndër-Amerikane për parandalimin, ndëshkimin dhe çrënjësjes e dhunës ndaj grave (Konventa Belém do Para)
5. Herring, Susan C. (2002). “Cyber Violence: Recognizing and Resisting Abuse in Online Environments. *Asian Women* 14 (Summer): 187-212, Indiana University, Bloomington USA.
6. Scottish Government (2020) Preventing violence against women and girls - what works: evidence summary.
7. Eige (European Institute for Gender Equality (2022b), ‘Cyber violence against women’,
8. Opinion on combatting online violence against women, European Commission Advisory Committee on Equal Opportunities for Women and Men, April 2020.
9. F. Di Tano, I reati informatici e i fenomeni del cyberstalking, del cyberbullismo e del revenge porn, in Th. Casadei, S. Pietropaoli [a cura di], Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, Wolters-Kluwer, Cedam giuridica, Milano, 2021,
10. Edoardo Buffagni “La cyberviolenza è una forma di violenza domestica: come affrontarla”Pubblicato il 10 Feb 2022, La cyberviolenza è una forma di violenza domestica: come affrontarla - Agenda Digitale,.
11. Th. Casadei, Corpi, soggetti, reti: una mappa sommaria delle sfide del presente, in Gf. Zanetti – Th. Casadei, Manuale di filosofia del diritto)
12. Frank H. Easterbrook, Cyberspace and the Law of the Horse, 1996 U. CHI. LEGAL F. 207. The reference is to an argument by Gerhard Casper, who, when he was dean of the University of Chicago Law School, boasted that the law school did not offer a course in “The Law of the Horse.” Id. at 207 (internal quotation marks omitted). The phrase originally comes from Karl Llewellyn, who contrasted the U.C.C. with the “rules for idiosyncratic transactions between amateurs.” Id. at 214.
13. V. Colomba, I diritti nel Cyberspazio. Architetture e modelli di regolamentazione. Con un saggio di Lawrence Lessing, Diabasis, Parma, 2015, pp. 75 e ss., in part. fq. 81
14. Edoardo Buffagni “La cyberviolenza è una forma di violenza domestica: come affrontarla”Pubblicato il 10 Feb 2022, La cyberviolenza è una forma di violenza domestica: come affrontarla - Agenda Digitale,.
15. Citron, Danielle K. *Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace*. University of Maryland Francis King Carey School of Law Legal Studies Research Paper, No. 2017-9, 2. See also “the Disturbing Rise of Cyberattacks against Abortion Clinics” in WIRED (10 May 2017)
16. El Asam, Aiman; Samara, Muthanna. *Cyberbullying and the law: A review of psychological*

- and legal challenge*. Computers in Human Behavior 65 (2016) 127-141.
17. <http://www.coe.int/en/web/children/bullying> (link last checked on April 3rd 2017).
 18. Tokunaga, Robert S. *Following you home from school: A critical review and synthesis of research on cyberbullying victimization*. Computers in Human Behavior, 26(3), 278.
 19. Van Leeuwen, J.C. Literature review on the research on cyberbullying definitions. Universiteit Twente. (2012).
 20. Moore, Michael J.; Nakano Tadashi; Enomoto Akihiro; Suda Tatsuya. *Anonymity and Roles Associated with Aggressive Posts in an Online Forum*. Computers in Human Behavior (2012).
 21. Juvonen, Jaana; Gross Elisheva F. *Extending the School Grounds?-Bullying Experience in Cyberspace*. Journal of School Health. Vol. 78(9). (2008), 496-505.
 22. Besley, Bill. Published on <http://www.cyberbullying.ca/> (link last checked 5th of April 2017).
 23. Smith, Peter K.; Mahdavi Jess; Carvalho Manuel; Fisher Sonja; Russell Shanette; Tippett Neil. *Cyberbullying: its nature and impact in secondary school pupils*. The Journal of Child Psychology and Psychiatry. Vol. 49(4). (2008), 376-385.
 24. Kowalski, Robin M.; Limber, Susan P. *Electronic Bullying Among Middle School Students*. Journal Of Adolescent Health 41 (2007) S22-S30. Erdur-Baker, Özgür. *Cyberbullying and its correlation to traditional bullying, gender and frequent and risky usage of internet-mediated communication tools*. New Media & Society. Vol. 12(1). (2009), 109-125.
 25. Clark, Marilyn/Grech, Anna (2017): Journalists under Pressure. Unwarranted interference, fear and self-censorship in Europe. Council of Europe Publishing. Strasbourg. PAASONEN, Sussanna. *Labors of love: netporn, Web 2.0 and the meanings of amateurism*. New Media & Society 12(8) 1297–1312.
 26. ERNI, John Nguyet. *Sex/Text: Internet Sex Chatting and “Vernacular Masculinity” in Hong Kong*. International Proceedings of Economics Development and Research, Vol. 44, 56-60.
 27. Marcum, Catherine D.; Higgins, George E.; Ricketts, Melissa L., *Juveniles and Cyber Stalking in the United States: An Analysis of Theoretical Predictors of Patterns of Online Perpetration*. International Journal of Cyber Criminology, Vol. 8, Issue 1, 48.
 28. Woodlock, Delanie (2016): *The Abuse of Technology in Domestic Violence and Stalking*. Violence Against Women. Volume: 23 issue: 5, page(s): 584-602
 29. Council of Europe/Data Protection and Cybercrime Division (2012): Protecting children against sexual violence: the criminal law benchmarks of the Budapest and Lanzarote Conventions (Discussion paper), Strasbourg, December 2012.
 30. Establishment of Harmonized Policies for the ICT (2012) Market in the ACP Countries, Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean.

31. Jurisprudencë e GJEDNJ:

- Çështja e Buturugă v. Romania (application no. 56867/15). ECHR 056 (2020) 10.02.2020.
- Çështja e Volodinës vs. Rusisë 14/12/2021

- Çështja KU kundër Finlandës , nr 2872/02/ 2008.
- Çështja Opuz kundër Turqisë , nr. 33401/02 ,ECHR 2009, dhe
- Çështja Bălşan k. Rumania , nr.49645 /09, 23 maj 2017
- Çështja Eremia v. the Republic of Moldova Nr. 3564/11 28/08/2013
- Çështja Söderman v. Sweden (nr. 5786/08), ECHR 333 (2013) 12.11.2013

Link:

- <http://journals.sagepub.com/doi/full/10.1177/1077801216646277> <https://www.wearethorn.org/sextortion/1880/>
 - <https://www.wired.com/2017/03/medical-devices-next-security-nightmare/>
 - <https://www.justice.gov/usao-md/pr/british-and-american-men-indicted-swatting>; <https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1>;
 - <https://www.fbi.gov/contact-us/field-offices/minneapolis/news/press-releases/houston-texas-area-teenager-sentenced->
 - <http://luxembourgguidelines.org/english-version/>
 - <https://www.cybercivilrights.org/revenge-porn-laws/>
 - <https://www.thelocal.de/20140522/court-forces-ex-lovers-to-delete-sexy-photos>
 - https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=3271AC-8D94E47247A2CFDC0389186E84.tpdila17v_1?idArticle=JORFARTI000033203291&cid-Texte=JORFTEXT000033202746&dateTexte=29990101&categorieLien=id
 - <http://www.legislation.gov.uk/ukpga/2015/2/section/33>
 - <https://www.wired.com/story/track-location-with-mobile-ads-1000-dollars-study/>
 - <https://www.wired.com/story/cyberattacks-against-abortion-clinics/>
 - <https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence>
 - <https://www.coe.int/en/web/cyberviolence>
 - <https://www.gov.scot/publications/works-prevent-violence-againstwomen-girls-summary-evidence/pages/6/>. Accessed 14 March 2023.
 - <https://eige.europa.eu/gender-based-violence/cyber-violence-against-women>
 - <http://www.un.org/womenwatch/daw/vaw/v-overview.htm> .
32. <https://www.coe.int/en/web/cyberviolence>



**SHKENCAT
E
APLIKUARA
DHE
EKONOMIKE**

SEKSIONI 3

