ActiveWatch

FreeEx Digest

- ediția nr. 2

Controlul și cenzura comunicațiilor digitale

Kingdom of the Netherlands

Proiectul FreeEx Digest este finanțat de Ambasada Regatului Țărilor de Jos. Opiniile și informațiile transmise în cadrul proiectului nu reprezintă poziția Ambasadei Regatului Țărilor de Jos. Responsabilitatea privind acuratețea informațiilor și deciziile editoriale sunt sub controlul exclusiv al Asociației ActiveWatch.

FreeEx Digest este un proiect editorial al Asociației ActiveWatch, realizat de echipa ActiveWatch și colaboratorii săi și susținut financiar de Ambasada Regatului Țărilor de Jos.

În următoarele luni vom produce periodic sinteze ale principalelor subiecte care pot influența negativ dreptul la informare corectă și libertatea de expresie în România.

Vom vorbi despre cazurilor unor jurnaliști care nu sunt lăsați să-și desfășoare activitatea în interes public, vom expune practici și instituții care restrâng libertatea de expresie și vom încerca să oferim recomandări și soluții pentru cetățenii copleșiți de fluxul uriaș de informații contradictorii sau înșelătoare care ne alimentează anxietatea și ne împiedică să luăm decizii în cunoștință de cauză.

Proiectul FreeEx Digest este inspirat de munca de peste 20 de ani dedicată monitorizării libertății presei și cuprinsă în rapoartele anuale privind libertatea de exprimare în România.

FreeEx Digest nr. 1 „Siguranța jurnaliștilor. Linșaj public și kompromat" poate fi citit aici.

FreeEx Digest nr. 2 a fost redactat în colaborare cu Asociația pentru Tehnologie și Internet (ApTI).

Premierul Ciucă referitor la interzicerea TikTok pe telefoanele instituțiilor din România:

„(...) **prin acest canal sunt livrate o serie întreagă de elemente, de mesaje care nu întotdeauna au conţinutul pe care ni-l dorim**.”

(martie 2023)

CUPRINS

FreeEx 2022 - 2023 // Controlul și cenzura comunicațiilor digitale

Săptămâna trecută, pe 28 februarie 2023, Curtea Constituțională a respins plângerile de neconstituționalitate formulate de partidele de opoziție și Avocatul Poporului pe marginea legii privind securitatea cibernetică. Legea fusese criticată de mai multe organizații neguvernamentale, inclusiv pentru că introduce „propaganda și dezinformarea" în lista amenințărilor la adresa siguranței naționale și impune obligații de securitate pentru toate „persoanele fizice și juridice care furnizează servicii publice ori de interes public", ceea ce, teoretic, poate include cu brio orice mass-media din domeniul online.

În contextul recentei decizii a Curții Constituționale, credem că merită să facem o sinteză a principalelor evenimente și inițiative legislative din domeniul comunicațiilor digitale, adoptate sau discutate de autorități pe parcursul ultimului an și jumătate, și care pot avea impact asupra activității jurnaliștilor. Or, siguranța jurnaliștilor include și confidențialitatea comunicațiilor și protecția vieții private online, Comisia Europeană solicitând țărilor membre să se asigure că jurnaliștii și ceilalți profesioniști din domeniul mass-media nu fac obiectul urmăririi sau al supravegherii online ilegale, inclusiv în contextul unor investigații ale poliției care pot compromite protecția surselor jurnalistice (vezi și ediția din februarie 2023 a FreeEx Digest nr. 1: „Siguranța jurnaliștilor. Linșaj public și kompromat").

Războiul din Ucraina a fost folosit pe parcursul ultimului an, de autoritățile statului, pentru a limita drepturi fundamentale, inclusiv libertatea de exprimare. Astfel, în 2022 au fost adoptate mai multe legi ce vizează comunicațiile digitale și care dau puteri sporite de acces la date nepublice serviciilor de informații, dar și dreptul de a interfera cu libertatea de exprimare. Dacă le privim din situația specifică a unui jurnalist sau redacții, aceste modificări legislative sunt cu atât mai îngrijorătoare. Criticile formulate de organizații cu expertiză în drepturi digitale, drepturi fundamentale și bună guvernare, de politicieni din opoziție și instituții europene, au fost în cea mai mare parte ignorate, Guvernul și Parlamentul lăsând impresia că răspund fără prea multă analiză critică cerințelor formulate de serviciile de informații. În majoritatea lor covârșitoare, noile prevederi legale au trecut, din păcate, testul de constituționalitate.

Războiul din Ucraina a intensificat și acțiunile de cenzură guvernamentală, dar și atacurile cibernetice, care au afectat și site-uri media. La aceasta s-au adăugat situațiile în care rețelele de socializare cenzurează sau limitează conținut într-un mod lipsit de transparență și pe baza unor algoritmi neclari. Astfel, statul, alături de actori privați, au îngrădit dreptul la informare al publicului.

Principalele evenimente și acțiuni cu impact asupra libertății comunicațiilor digitale în 2022 - 2023:

Serviciile de informații își scriu singure legile

Autoritățile de la București au iscat puternice controverse publice în iunie 2022, când în presă s-au scurs informații despre un pachet de legi ale securității naționale, despre care se presupune că nu ar fi fost redactat în birourile Guvernului României, cum ar fi fost firesc, ci, mai degrabă, în cele ale serviciilor de informații. Principala problemă a acestui pachet de legi ale securității naționale era aceea că dădea puteri sporite pentru serviciile de informații, în timp ce controlul asupra acestor servicii era diminuat.

Legea securității cibernetice: mai multă Securitate, mai puțină siguranță

Conform noii legi a securității și apărării cibernetice, declarată constituțională de CCR pe 28 februarie 2023, persoanele fizice și juridice (deci, potențial, inclusiv mass-media) care furnizează servicii publice ori de interes public au obligații extinse, inclusiv de a raporta incidentele de securitate cibernetică care le-au afectat sistemele, în maximum 48 de ore de la producerea acestora, sau riscă o amendă contravențională usturătoare (1-3% din cifra de afaceri). De asemenea, furnizorii de servicii de securitate cibernetică sunt obligați să ofere informații despre securitatea clienților lor (deci inclusiv mass-media), în lipsa unui mandat judecătoresc și, chiar dacă informațiile solicitate sunt protejate de un contract de confidențialitate.

Una dintre cele mai grave prevederi o constituie completarea, prin noua lege, a unor prevederi din legea siguranței naționale, în vigoare. Astfel, campaniile de „propagandă sau dezinformare, de natură a afecta ordinea constituțională" se adaugă listei de amenințări la siguranța națională, ceea ce dă puteri nejustificate SRI în limitarea dreptului la libertatea de exprimare, prin stabilirea unilaterală a acțiunilor ce intră în această categorie, dar și a colectării de informații și efectuare de măsuri specifice de supraveghere în astfel de cazuri. Practic o întreagă redacție poate fi urmărită de SRI, doar dacă este bănuită că a fi responsabilă de acțiuni care sunt incluse în această categorie (legal, urmărirea se poate face doar cu mandat de la judecător, dar să nu uităm ca de facto acest filtru nu există - peste 99% din mandatele de supraveghere pe siguranță națională sunt aprobate).

Lărgirea interceptării comunicațiilor electronice

Modificările la codul comunicațiilor adoptate în 2022 au iscat la rândul lor controverse publice puternice, pentru că au lărgit nepermis posibilitatea interceptării comunicațiilor electronice de către organele de cercetare penală și SRI, impunând obligații excesive furnizorilor, inclusiv unei noi categorii de furnizori de servicii de găzduire electronică. În cazul presei, aceasta ar însemna că orice date (probe din investigații, articole nepublicate, informații trimise de avertizori de integritate, etc.), care ar fi pe un server, pot fi obținute direct de la găzduitor, în urma unui mandat trimis acestuia.

Cenzura guvernamentală - site-uri blocate arbitrar

Directoratul Național de Securitate Cibernetică (DNSC) cere să se blocheze site-uri fără a avea o bază legală clară, fără procedura de apel și fără a îndeplini criteriile necesare de independență instituțională. Blocarea unui site de presă (aktual24.ro), precum și a unui blog de recenzie de carte și a site-urilor unor magazine, inclusiv a unor adrese IP aflate în proprietatea Google, dau măsura arbitrariului acestui tip de acțiune, inițiată ca o extindere a blocării site-urilor oficiale rusești cerută de Uniunea Europeană.

Cenzura privată

Blocarea, limitarea sau ștergerea de pe rețele de socializare a conturilor mass-media în limba română - fără explicații sau vreun motiv legal, urmate deseori de imposibilitatea de a le relua și a recupera audiența avută - este o practica curentă a Facebook și/sau Google de mulți ani. Măsurile par fi luate fie de sisteme automatizate, fie de persoane care nu înțeleg limba română la nivel primar. Astfel de măsuri au afectat, în ultimii ani, paginile mai multor publicații online, cum ar fi: HotNews, G4Media, profit.ro, Aktual24.ro, Dela0, Investigatoria, descopera.ro. Pagina Facebook a publicației de satiră Times New Roman a fost ștearsă. Și jurnaliștii au fost afectați de deciziile arbitrare ale Facebook. De exemplu, nu mai departe de ianuarie 2023, pagina lui Cătălin Tolontan și-a diminuat brusc reach-ul după publicarea unui link referitor la o investigație Libertatea care viza un agresor sexual.

Atacuri informatice asupra mass-media

În contextul războiului din Ucraina, numărul atacurilor cibernetice a crescut, multe dintre ținte fiind site-urile unor redacții. Site-urile Digi24, Hotnews și G4Media au fost afectate de astfel de atacuri.

Serviciile de informații au început 2023 cu puteri sporite, în detrimentul protejării drepturilor fundamentale ale cetățenilor și a existenței unui echilibru al puterilor în stat. Ne putem aștepta că acest trend va continua, în condițiile în care controlul civil asupra serviciilor de informații nu preocupă în mod real decât o mână de politicieni, de obicei din opoziție, și câteva organizații ale societății civile, iar controlul judecătoresc este de facto inexistent. Conform pachetului de legi ale securității menționat la început, controlul parlamentar asupra serviciilor de informații s-ar putea diminua semnificativ. Marja mai largă de acțiune a serviciilor de informații are un potențial impact și asupra libertății de exprimare și a libertății presei, pentru că siguranța comunicațiilor jurnaliștilor este diminuată, odată cu cea a oricărui cetățean. Să mai adăugăm la aceasta și că au trecut doar șase ani de când SRI a recunoscut că are agenți infiltrați în presă, informație întărită de un fost director SRI. Serviciile de informații își scriu singure legile.

Legile securității

Începând cu finalul lunii mai 2022, G4Media a făcut public faptul că pe masa coaliției de guvernare se afla un set de zece proiecte de legi ale securității. Nevoia de modernizare a legislației din domeniu este indiscutabilă, însă pachetul de legi prezentat de G4Media a scos la iveală girul coaliției de guvernare pentru reducerea semnificativă a controlului civil asupra serviciilor de informații. Acestea (în special SRI și SIE), conform proiectelor de lege, ar urma să primească drepturi lărgite. Publicarea proiectelor a declanșat un scandal public, deși multe redacții l-au ignorat complet sau chiar au ridicat suspiciuni că cenzurează subiectul. Astfel, conform proiectelor de lege scurse către presă:

- SRI poate cere sprijinul cetățenilor oricând ar considera că are nevoie, iar aceștia ar fi obligați să îl ajute. Fără excepții. Inclusiv, deci, jurnaliștii.

- Procurorii ar putea desfășura percheziții în sediile SRI și SIE doar cu aprobarea președintelui CSAT (care este Președintele României) și doar dacă directorul serviciului a fost anunțat înainte. Mai mult, doar anumiți procurori desemnați ar putea ancheta ofițerii serviciilor de informații.

- Lista domeniilor care constituie amenințări la securitatea națională s-ar mări, incluzând crima organizată, infrastructuri critice de comunicații și tehnologia informațiilor, interesele științifice și de cercetare ale României, sistemul de administrație publică, sănătate, educație și patrimoniul cultural. Practic, prin extinderea listei domeniilor care vizează siguranța națională într-un mod atât de larg, SRI ar putea solicita mandate de siguranță națională pentru orice motiv. Aceste mandate ar putea fi solicitate direct de la ICCJ, fără să mai fie nevoie să treacă prin Parchetul General.

- Controlul Parlamentului asupra serviciilor ar scădea. Directorul SRI ar mai putea fi demis doar de Președintele României, pe motiv de implicare în politică. Parlamentul nu ar mai putea cere demiterea directorului, ci doar ar vota numirea în funcție. Serviciul s-ar bucura și de mai multă libertate în ceea ce privește activitățile sub acoperire. În prezent companiile deschise de SRI sunt sub control parlamentar, control de care ar scăpa prin acest proiect. De asemenea, directorul instituției nu ar mai fi obligat să prezinte un raport anual Parlamentului.

Acestea nu sunt singurele probleme pe care le ridică pachetul de legi dezvăluit de presă. În cele zece proiecte de legi cuprinse în pachetul neasumat oficial de Guvern există nenumărate articole care încalcă în mod direct drepturi fundamentale, precum libertatea de exprimare sau dreptul la viață privată. Mai mult, proiectele încearcă să recupereze din atribuțiile SRI pierdute sau puse sub semnul întrebării prin decizii ale CCR.

Nicio persoană și nicio instituție nu și-a asumat scrierea acestor proiecte de lege. Premierul Ciucă a afirmat vag că „legile au fost elaborate la nivelul fiecărei instituții

responsabile în parte". Marcel Ciolacu a spus și el că știa de existența legilor. Președintele Klaus Iohannis a negat faptul că el a văzut proiectele, în ciuda faptului că SIE a declarat că „variantele de lucru ale legilor securității naționale sunt rezultatul consultărilor cu Administrația Prezidențială și Secretariatul General al Guvernului". Mai mulți parlamentari au acuzat serviciile că au scris pachetul de legi.

În prima sa reacție, Președintele Klaus Iohannis a fost mai îngrijorat de modul în care proiectele au devenit publice decât de conținutul acestora. Mai mult, el l-a amenințat voalat pe avertizorul de integritate care a dat presei documentele.

45 de ONG-uri, printre care Asociația pentru Tehnologie și Internet și ActiveWatch, au criticat atât declarația Președintelui, cât și pachetul de legi. Și organizația Reporteri fără Frontiere a condamnat reacția șefului statului, care i-a amenințat pe jurnaliștii de la G4Media și sursa lor.

Deși pachetul de legi ar fi trebuit să intre pe agenda guvernului în vara anului 2022, scandalul public din jurul acestora a dus la amânarea adoptării lor. Parlamentul a adoptat până la finalul anului 2022 un proiect dintre cele zece, respectiv legea securității și apărării cibernetice.

Legea securității cibernetice

Ministerul Cercetării, Inovării și Digitalizării a inițiat la începutul lunii noiembrie 2022 un proiect de lege privind securitatea și apărarea cibernetică a României. Acesta face parte din pachetul neoficial de legi ale securității naționale, fiind aproape identic cu cel prezentat de G4Media la începutul verii. Versiunea adoptată de Guvern a fost modificată față de cea care s-a aflat în dezbatere publică, fiind mai dură (s-a introdus un capitol întreg de sancțiuni - cu amenzi până la 10% din cifra de afaceri) și mai extinsă (alineatul cu propaganda și dezinformarea a fost inclus în lege abia la momentul adoptării de către Guvern).

Ulterior, proiectul de lege a fost adoptat de Parlament, în decembrie 2022, trecând prin ambele camere în numai nouă zile. CCR s-a pronunțat asupra constituționalității proiectului de lege în 28 februarie 2023, în urma formulării unor plângeri de neconstituționalitate, de către Avocatul Poporului și, respectiv, USR și Forța Dreptei.

Conform legii privind securitatea și apărarea cibernetică, urmează să se înființeze Sistemul Național de Securitate Cibernetică (SNSC), care se va afla sub managementul Consiliului Operativ de Securitate Cibernetică (COSC). SNSC este un cadru pentru cooperarea dintre 12 instituții: CSAT, MCID, DNSC, ANCOM, MApN, MAI, MAE, ORNISS, SRI, SIE, STS și SPP. COSC este un organ consultativ, președintele fiind consilierul prezidențial pentru probleme de securitate națională. SRI are în responsabilitate secretariatul tehnic.

Atât Asociația pentru Tehnologie și Internet (ApTI), cât și APADOR-CH au criticat unele dintre prevederile legii, critică la care s-au raliat mai multe organizații. Organizațiile neguvernamentale au afirmat că noua lege va extinde în mod nejustificat responsabilitățile de protejare a securității cibernetice către categorii largi de companii și persoane. Serviciile ar avea posibilitatea să restrângă arbitrar și, deci, potențial abuziv, drepturi fundamentale, cum ar fi drepturile la viață privată și la libertatea de exprimare.

Conform noii legi, persoanele fizice și juridice care furnizează servicii publice ori de interes public au obligația de a raporta incidentele de securitate cibernetică, în maximum 48 de ore de la producerea acestora, prin Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC), unde au acces 11 instituții dintre cele precizate mai sus. Conform ApTI, aceasta excede cadrului juridic european. Practic, orice furnizor de internet şi deținătorul oricărei rețele sau sistem informatice din mediul privat, considerate de interes public, deci potențial orice instituție de presă, ONG sau entitate privată care furnizează servicii publice ori de interes public, ar putea cădea sub incidența legii. Termenii folosiți nu sunt definiți în lege (în ciuda observațiilor formulate în acest sens de mai multe organizații), astfel încât va rămâne la latitudinea autorităților să decidă, prin legislație secundară subsecventă (deci potențial a fi modificată de către orice guvern), cine vor fi acești „furnizori de servicii publice ori de interes public". ApTI și APADOR-CH au arătat că pentru multe companii mici va fi imposibil să respecte termenul de 48 de ore, la fel ca și alte obligații pentru acești furnizori, cum ar fi cea de analiză de risc a lanțului

de aprovizionare. Amenzile contravenționale impuse de noua lege sunt disproporționat de mari - de la 1% din cifra de afaceri pentru prima abatere (!) până la 3% din cifra de afaceri la a doua abatere.

O altă problemă o ridică obligația impusă furnizorilor de servicii de securitate cibernetică de a oferi informații despre securitatea clienților lor către 11 instituții, în lipsa unui mandat judecătoresc, și doar pe baza unui „cereri motivate". De exemplu, o instituție precum ORNISS sau MApN sau MCID are dreptul să primească răspunsuri la orice întrebări formulează către un furnizor de securitate cibernetică, chiar dacă datele solicitate sunt protejate de un contract de confidențialitate. După cum a explicat ApTI, această obligație reprezintă o încălcare a confidențialității contractuale similară ca și concept cu cea în care avocatul ar fi obligat să furnizeze informații despre ce face clientul său, un jurnalist despre sursele sale ori un auditor contabil despre clienții săi.

Una dintre cele mai grave prevederi o constituie completarea, prin noua lege, a unor prevederi din legea siguranței naționale, în vigoare. Astfel, campaniile de „propagandă sau dezinformare, de natură a afecta ordinea constituțională" se adaugă listei de amenințări la siguranța națională, ceea ce dă puteri nejustificate SRI, în limitarea dreptului la libertatea de exprimare. După cum arată analiza organizațiilor neguvernamentale, deoarece campaniile de „propagandă sau dezinformare" nu sunt suficient de limitativ definite de lege, rămâne la latitudinea unei autorități precum SRI să decidă ce se circumscrie definiției din lege. Prin această modificare legislativă, arată organizațiile menționate, ar putea deveni infracțiune inclusiv formularea de opinii contrare unei politici oficiale a statului (de exemplu politica de vaccinare). Astfel, autorilor unor astfel de poziții critice, îndreptate împotriva politicii oficiale, sau, în general, oricăror persoane responsabile de orice campanii pe care SRI le-ar considera „propagandă sau dezinformare, de natură a afecta ordinea constituțională", li se pot deschide procese penale, aplicându-se art. 404 din Codul penal: „Comunicarea sau răspândirea, prin orice mijloace, de ştiri, date sau informaţii false ori de documente falsificate, cunoscând caracterul fals al acestora, dacă prin aceasta se pune în pericol securitatea naţională, se pedepseşte cu închisoarea de la unu la cinci ani." În plus, prin introducerea campaniilor de „propagandă sau dezinformare, de natură a afecta ordinea constituțională" în lista de amenințări la siguranța națională, SRI poate solicita mandate de supraveghere pe siguranță națională pentru orice măsură de supraveghere tehnică în vederea depistării sau analizei acestor cazuri.

Codul comunicațiilor

Codul european al comunicațiilor este o directivă europeană din 2018, care în România a fost pregătită de aplicare încă din noiembrie 2020. Aceasta a fost adoptată însă un an mai târziu, cu trei zile înainte ca Guvernul Cîțu să fie demis.

Legea, în forma propusă de Guvern, venea cu un articol problemă, suplimentar textului european, și care nu existase în proiect în perioada în care se afla în dezbatere publică: art. 10^2. Acest articol lărgea spectrul interceptării comunicațiilor electronice, inclusiv la conținutul comunicațiilor criptate.

Proiectul ar fi afectat două tipuri de furnizori:

- furnizorii de găzduire electronică cu resurse IP (cei care asigură servicii de acces la conținut stocat pe o adresă web - practic tot ceea ce este pe web),
- furnizorii de servicii de comunicații interpersonale care nu se bazează pe numere (aplicații precum WhatsApp, Messenger, Signal sau Telegram).

În urma criticilor aduse de opoziție și de ONG-uri (în principal ApTI), cea de-a doua categorie a fost scoasă înainte de votul Senatului, de la începutul anului 2022 (Camera Deputaților votase proiectul la finalul lui 2021). Astfel, doar furnizorii de găzduire electronică cu resurse IP rămân afectați.

Conform art. 10^2, acest tip de furnizori trebuie să ajute organele statului în monitorizarea tehnică a clienților și utilizatorilor lor. Mai exact, obligațiile sunt detaliate în patru domenii, explicate vag:

- a) să permită interceptarea legală a comunicaţiilor, inclusiv să suporte costurile aferente;
- b) să acorde accesul la conţinutul comunicaţiilor criptate tranzitate în reţelele proprii;
- c) să furnizeze informaţiile reţinute sau stocate referitoare la date de trafic, date de identificare a abonaţilor sau clienţilor, modalităţi de plată şi istoricul accesărilor cu momentele de timp aferente; (acest punct a fost declarat neconstitutional, și eliminat din forma finală a legii - vezi mai jos)
- d) să permită, în cazul furnizorilor de servicii de găzduire electronică cu resurse IP, accesul la propriile sisteme informatice, în vederea copierii sau extragerii datelor existente.

O altă problemă creată de proiect în lit. a) este că furnizorii, și nu statul, sunt responsabili de construirea și întreținerea infrastructurii de interceptare. De asemenea, toți furnizorii de găzduire sunt obligați să se înregistreze la ANCOM. Conform ApTI, aceasta contrazice legislația europeană, anume directiva e-commerce.

Proiectul a trecut de Parlament și a fost contestat la Curtea Constituțională de către Avocatul Poporului și USR. CCR a declarat neconstituțională doar litera c). În 6 iulie 2022, Președintele României a promulgat legea, după ce aceasta a trecut de Parlament modificată.

Aproape nouă luni de la promulgare și ANCOM nu are nicio procedură și niciun registru public în care furnizorii de găzduire se pot notifica și niciun proiect public în acest sens (spre deosebire de ceilalți furnizori reglementați deja).

Cenzura guvernamentală - site-uri blocate arbitrar

Invazia militară rusă din Ucraina a reprezentat pentru autoritățile din domeniile siguranței Internetului un nou pretext pentru a lua decizii arbitrare de blocare a unor site-uri, în baza unui cadru legal inexistent. Mai mult, autoritățile nu par să fi învățat lecțiile din pandemie, când, în numele combaterii dezinformării, au luat decizii controversate care au alimentat și mai mult neîncrederea la nivelul opiniei publice și au legitimat tocmai acele voci care aderă la teorii ale conspirației, în detrimentul unor dezbateri transparente și deschise.

Blocarea unui site, care este un mijloc de comunicare publică, reprezintă o decizie sensibilă pentru că echivalează cu suprimarea unei publicații de la apariție, deci cu încălcarea unui drept fundamental și constituțional. Într-un stat democratic, o acțiune de acest fel poate fi acceptabilă doar ca o soluție extremă. O asemenea decizie trebuie să fie luată cu transparență, cu informarea celor vizați și pe o bază legală clară, care să permită accesul la foruri independente de revizuire a acesteia. În orice situație, trebuie urmate cerințele CEDO pe acest subiect, care are o largă jurisprudență în acest sens.

Pe 28 februarie 2022, mai multe surse acuzate de propagandă rusă au fost blocate, printre care și Sputnik și Russia Today. Decizia de a stopa cele două canale media a fost luată la nivel european (printr-o decizie a Consiliului European) și ulterior lărgită la alte patru site-uri din Rusia.

În aceeași zi, Directoratul Național de Securitate Cibernetică (DNSC) a publicat o listă cu site-uri de „fake-news" și cu adrese IP folosite la atacuri cibernetice. Într-un comunicat de presă din aceeași zi, instituția a admis că „problematica <<fake news>> nu se află în atribuțiile Directoratului". În fapt, legal vorbind, DNSC nu poate decide asupra blocării unui site. Pe teritoriul României, blocarea site-urilor s-a făcut prin furnizorii de internet, care sunt reglementați de ANCOM.

În 3 martie 2022, Asociația pentru Tehnologie și Internet (ApTI), alături de alte câteva organizații, trimis o scrisoare nepublică către DNSC și ANCOM, prin care au cerut aplicarea mai multor măsuri care să prevină abuzul. Scrisoarea a rămas fără răspuns. Mai grav, tot pe 3 martie, lista menționată mai sus a fost extinsă cu două domenii, unul dintre acestea era aktual24.ro, o publicație online lansată în 2015 de către jurnalistul Ovidiu Albu. Blocarea site-ului a avut loc fără ca ziaristul să fie avertizat în vreun fel de către autorități de această decizie. Albu a negat pe pagina personală de Facebook acuzațiile de propagandă pro-rusă și a subliniat că, dimpotrivă, poziția aktual24.ro fusese critică față de invazia Rusiei în Ucraina.

Abia după o zi, pe 4 martie, în contextul scandalului public iscat de blocarea site-ului, aktual24.ro a început să funcționeze din nou. Totuși, nicio instituție nu a explicat decizia de a include site-ul în lista celor blocate. Mai mult, DNSC a afirmat

într-un comunicat de presă că decizia de blocare nu îi aparține, listele publicate zilnic și transmise către autoritățile statului fiind un efort colaborativ coordonat între mai multe instituții ale statului, cu competențe în domeniu.

În 15 martie 2022 în spațiul public a apărut informația că blocările ilegale de site-uri au continuat. Printre zecile de domenii afectate s-au numărat: bookblog.ro, un blog de recenzii de carte; doilupi.ro, un magazin din Beiuș; enterieur.ro, un site de mobilă; două subdomenii firebaseio.com, deținute de Google. La presiunea societății civile, DNSC și-a motivat acțiunile, invocând o alertă internațională conform căreia aceste site-uri ar fi fost implicate în atacuri DDoS asupra unor instituții UE.

Ultima lista actualizată de DNSC în septembrie 2022 conținea peste 36.000 de IP-uri, din care majoritatea erau din SUA. O parte semnificativă dintre acestea sunt TOR exit nodes, folosite inclusiv de jurnaliști și activiști din țări unde Internetul este cenzurat (de ex. Belarus, Rusia, China) pentru a putea accesa conținut blocat în țara lor.

Cenzură privată

O altă problemă care a continuat în 2022 au fost restricțiile impuse jurnaliștilor de către companiile de social media.

Pagina de Facebook a publicației de satiră Times New Roman, care avea 13 ani de existență, 650.000 de urmăritori și peste 30.000 de postări, a fost ștearsă.

Pagina de Facebook a site-ului Investigatoria a fost raportată în masă, ceea ce a rezultat în ștergerea mai multor postări. Potrivit Investigatoria, acest lucru s-ar fi întâmplat după publicarea unui articol care a dus la arestarea unui consilier județean suspectat de acte de pedofilie. De asemenea, pagina publicației profit.ro a fost restricționată, astfel încât postările nu au mai putut fi sugerate utilizatorilor, situație cu care și Aktual24 s-a confruntat în 2022. De altfel, Facebook a mai restricționat în trecut paginile mai multor redacții, printre care și G4Media, HotNews, Dela0, descopera.ro (o revistă de istorie), dar și conturile unor jurnaliști, persoane publice sau politicieni.

La începutul anului 2023, jurnalistul Cătălin Tolontan a anunțat că pagina sa de Facebook și-a diminuat reach-ul după ce a publicat link-uri la investigațiile ziarului Libertatea legate de un agresor sexual. Jurnalistul a relatat că acest lucru s-a întâmplat din cauză că algoritmii nu disting între a expune un agresor și a promova o agresiune.

Atacuri cibernetice

În contextul războiului din Ucraina, anul 2022 a văzut o creștere a numărului de atacuri cibernetice, majoritatea fiind atacuri informatice de tip DDoS. Acest tip de operațiune vizează site-urile și serverele și are ca scop epuizarea resurselor, prin foarte multe accesări într-un timp scurt.

În cazul României, majoritatea atacurilor au venit din partea unei grupări independente, dar pro-rusă - Killnet -, atacurile fiind mai intense la începutul invaziei. Gruparea pro-rusă a amenințat că vrea să atace 300 de site-uri, multe dintre acestea fiind site-uri media. În România, Killnet a revendicat atacuri DDoS atât asupra site-urilor unor redacții, precum Digi24, cât și asupra site-urilor unor instituții de stat: Guvernul României, Ministerul Apărării, DNSC, CFR, Poliția etc. HotNews a fost victima unui atac DDoS în mai 2022. Chiar dacă nicio grupare nu a revendicat acțiunea, suspectul principal a fost tot KillNet. Site-ul G4Media a suferit un atac DDoS în septembrie 2022. G4Media a asociat acest incident cu publicarea unui articol legat de plagiatul premierului Nicolae Ciucă. La acea dată, premierul a cerut public investigarea evenimentului.

Echipa

Andrei Boloș/ ActiveWatch

Ionuț Codreanu / ActiveWatch

Liana Ganea/ ActiveWatch

Ioana Popa / ActiveWatch

Bogdan Manolea /ApTI

Licență

Creative Commons CC-BY 4.0 (Attribution)

București,
Martie 2023