CZU 343.14

ADMINISTRAREA PROBELOR PRIN INTERCEPTAREA DE COMUNICĂRI ELECTRONICE ÎN PROBATORIUL PENAL

Elena CROITOR,
doctor în drept, lector superior (USM)

Whether it's performed by a cell phone or by any other device, the electronic communication is of utmost importance for the criminal justice system. The conversations made by these specific technical means bear various kinds of information, starting with content of the communication itself, and ending with the details that ensure the identification of the subject, its location, the IP address and some other relevant data necessary for a fair settlement of the criminal case. Therefore, when it comes to investigating activities effectiveness the interception of the electronic communications plays a central part.

Keywords: electronic communications; interception; instant messaging; chat; authorization; evidence.

Intensitatea intervenției comunicărilor electronice în activitatea socială cotidiană justifică interesul procedurii penale pentru monitorizarea şi controlul lor, precum şi pentru folosirea informaţiilor pe care le furnizează întru realizarea scopului probatoriului penal. În acelaşi sens, *Recomandarea nr. R(95)13 a Comitetului de Miniştri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaționale* [1] solicită jurisdicţiilor naţionale crearea unui fundament normativ care ar admite sechestrarea, percheziţionarea, interceptarea sistemelor informaţionale şi constituirea de probe electronice aplicabile nu numai pentru soluţionarea cauzelor penale la nivel naţional, dar şi pentru necesităţile cooperării juridice internaţionale.

Cu toate acestea, calitatea de secret ocrotit prin lege a conţinutului convorbirilor electronice, subliniat şi de actul internaţional menţionat, implică unele limitări ale procesului de administrare a respectivei probe, atât sub aspectul admiterii acestuia, cât şi din perspectiva admisibilităţii ulterioare a datelor obţinute. În plus, specificul naturii informaţiei, a procedurii prin intermediul căreia poate fi dobândită, a parametrilor tehnici ce urmează a fi respectaţi pentru a asigura admisibilitatea impun condiţii extrem de riguroase activităţii de strângere a probelor pe calea interceptării comunicărilor electronice.

Delimitări conceptuale. Reprezintă *comunicări electronice* orice comunicări realizate prin intermediul unui sistem informatic. Se consideră *sistem informatic,* în sensul *Convenţiei europene privind criminalitatea informatică* [2], orice dispozitiv izolat sau ansamblu de dispozitive interconectate sau aflate în legătură, care asigură, ori, dintre care, unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor. Altfel spus, *comunicarea electronică* este orice transfer al simbolurilor, semnalelor, textului, imaginilor, sunetelor, datelor sau informaţiilor de orice natură, realizat în tot sau în parte prin intermediul cablurilor, sistemelor electromagnetice, fotoelectronice sau fotooptice […].

Legislaţia şi practica unor state [3] exclud din această categorie orice comunicare pe fir, verbală, făcută prin intermediul unui dispozitiv care transmite doar tonuri de semnalizare, precum şi orice comunicare provenită de la un dispozitiv de urmărire a locaţiei şi informaţia privind transferul electronic al fondurilor, utilizată şi creată de o instituţie financiară. Excepţiile indicate s-ar datora, în mare parte, recunoaşterii normative exprese, în legislaţiile respective, a trei forme de comunicare – verbală, electronică şi prin cablu – fapt care determină excluderea lor reciprocă.

Prin *interceptare* (în sens tehnic) se înţelege acţiunea de a capta, cu ajutorul unui dispozitiv electronic, special fabricat în acest scop, sau a unui computer, impulsurile electrice, variaţiile de tensiune sau emisiile electromagnetice care tranzitează în interiorul unui sistem informatic sau se manifestă ca efect al funcţionării acestuia, ori se află pe traseul de legătură dintre două sau mai multe sisteme informatice care comunică [4, p.3]. *Interceptarea* se referă, de asemenea, la preluarea semnalului optic şi celui digital.

În RM, C.proc.pen. nu conţine vreo definiţie a comunicărilor electronice, a sistemului informatic sau unele clasificări ale acestora. Mai mult, actul normativ respectiv nu indică direct asupra interceptării comunicărilor electronice, reglementând în general, în contextul art. 132^8 şi 132^9, interceptarea şi înregistrarea comunicărilor. Indubitabil, interpretarea legii nu poate fi făcută decât în sensul admiterii monitorizării conţinutului tuturor formelor prezente şi ulterioare de comunicare prin intermediul mijloacelor tehnice, răspunzând, în acest fel, exigenţelor evoluţiei şi perfecţionării permanente a ultimelor. În acelaşi sens, CtEDO a statuat [5] că lipsa unei specificări exprese în textul legii a unor forme particulare de realizare a acţiunii procesuale, inclusiv menţiuni cu

privire la datele electronice, nu reprezintă, ca atare, o abatere de la cerinţa art. 8 CEDO – ingerinţă prevăzută de lege.

Îmbinând perspectivele tehnică şi juridică, se poate aprecia că *interceptarea comunicărilor electronice* presupune detectarea şi ascultarea, cu ajutorul mijloacelor tehnice, a conţinutului convorbirilor realizate în timp real prin intermediul unui sistem informatic.

Perspectiva tehnică. Din punct de vedere normativ, toate formele de interceptare a comunicărilor, indiferent de natura lor, sunt identice sub aspectul actelor procesuale şi procedurale necesare dobândirii, pe această cale, a probelor. În pofida faptului dat, particularităţile de ordin tehnic ale constituirii şi transmiterii datelor electronice impun condiţii suplimentare administrării probei prin procedeul probatoriu invocat, determinând, în acelaşi timp, necesitatea satisfacerii unor cerinţe aparte atât din punctul de vedere al formulării demersului judecătorului de instrucţie, cât şi din perspectiva soluţionării acestuia în sensul admiterii.

În primul rând, aceasta vizează delimitarea măsurii respective de investigaţie de cele asemănătoare sub aspectul informaţiei-scop, cum ar fi, spre exemplu, interceptarea comunicărilor şi prevederile art.132[6] al C.proc.pen. Art.133, în redacţia nouă a C.proc.pen., cu toate că se referă în alin. (2) şi la conversaţiile mijlocite de poşta electronică, prin descrierea ordinii procesuale de realizare, face imposibilă aplicarea acestei acţiuni de urmărire penală şi în privinţa datelor transmise prin intermediul serviciului enunţat. În schimb, art.134[1] C.proc.pen. conţine prevederi particulare pentru conexiunile electronice, devenind, astfel, temeiul normativ al verificării conţinutului unor forme particulare ale comunicărilor de acest gen şi, drept urmare, necesitând delimitare în raport cu *interceptarea comunicărilor* (electronice – *n.a.*). Criteriile determinante, în acest sens, sunt momentul realizării acţiunii procesuale, cel al comunicării propriu-zise, precum şi realizarea acesteia din urmă în timp real [6], similar tuturor celorlalte forme de înregistrare. Prezenţa indicatorilor sus-numiţi determină aplicabilitatea interceptării comunicărilor, lipsa lor – necesitatea recurgerii la prevederile art.134[1] C.proc. pen. RM. Astfel, dacă procesul penal este interesat de comunicarea definită ca un dialog sau monolog, ce se desfăşoară imediat şi coincide cu momentul în care se realizează şi măsura specială de investigaţie, nu se poate solicita şi admite o altă acţiune decât interceptarea convorbirilor electronice. În cazul în care se constată că importanţa probatorie pentru cauza penală, aflată în soluţionare, prezintă corespondenţa expediată sau primită de bănuit, învinuit, sau de persoanele indicate în art. 132[8] C.proc.pen., dar care este independentă de factorul de timp, în raport cu momentul realizării propriu-zise a comunicării, se poate proceda doar la monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice.

Pe de altă parte, deşi ambele măsuri speciale de investigaţi se referă, în sens larg, la corespondenţă [7, p.1310-1311], interceptarea se va face în raport cu informaţia transmisă prin intermediul programelor *instant messaging*, care asigură comunicarea în timp real, iar monitorizarea conexiunilor comunicaţiilor telegrafice şi electronice – în privinţa celei expediate prin poşta electronică. Unele pagini web pot oferi ambele posibilităţi – atât transmisiunea datelor de la un utilizator sau altul în regim direct, cât şi expedierea fără o aşteptare rezonabilă a autorului la un răspuns momentan, considerent din care este imperativ ca actul prin care se solicită şi cel prin care se admite aplicarea unuia din aceste două procedee probatorii să identifice exact corespondenţa care urmează a fi supravegheată şi datele care pot fi preluate, „citite", expediate, re-expediate etc.

Convorbirile electronice în timp real, la rândul lor, au, din punct de vedere tehnic, două forme de manifestare: *singular instant messaging,* care presupune o comunicare între un expeditor şi un destinatar al datelor şi *multiple instant messaging*, caracterizată de posibilitatea comunicării concomitente între unul sau mai mulţi expeditori şi/sau destinatari.

Importanţa practică a delimitărilor se determină în raport de caracterul şi gradul prejudiciabil al cauzei, de probabilitatea obţinerii informaţiilor şi relevanţa lor pentru cauză depinde aprecierea proporţionalităţii intervenţiei în viaţa privată şi autorizarea măsurii date de investigaţie. În plus, motivarea şi întemeierea demersului înaintat în acest sens trebuie să se facă reieşind din materialul probant care confirmă oportunitatea dispunerii interceptării comunicărilor electronice.

La etapa actuală, orice utilizator al serviciilor internet poate descărca versiuni gratuite sau contra plată a programelor care să asigure comunicarea în timp real (Skype, WhatsApp, Snapchat, Viber, Pidgin, WeChat, Slack, Facebook Messenger etc.), sau să le acceseze pe cele integrate în paginile web, cu formarea unei pseudoidentităţi necesare înregistrării şi utilizării serviciului, fie cu folosirea aceleiaşi identităţi create anterior pentru site-ul prin intermediul căruia se face comunicarea. Totodată, este posibilă înregistrarea prin intermediul numărului de telefon, precum există şi servicii fără înregistrare, dar care nu privează subiectul oficial de posibilitatea de identificare, cel puţin a punctului de acces la sistemul informatic sau, eventual, a unei adrese IP.

Perspectiva tehnică a preluării informaţiei computerizate transmise de un utilizator altuia instantaneu nu se limitează însă la stabilirea tipului de comunicare sau a programului care asigură convorbirea,

ci vizează, de asemenea, şi mijlocul tehnic/sistemul informatic prin intermediul căruia se face comunicarea, adică personal computer, notebook, tabletă sau telefon mobil etc., precum şi datele de identificare a celor din urmă. Sub acest din urmă aspect, pentru a asigura rezonabilitatea intervenţiei în drepturile fundamentale, prin recurgerea la procedeul probatoriu dat şi pentru a stabili limitele lui certe, sunt necesari parametri după care să se facă identificarea. În unele cazuri, se recurge la indicatori stabiliţi în raport cu tehnica de calcul care asigură comunicarea, cum ar fi adresa IP sau adresa fizică, sau în funcţie de serviciul care mijloceşte comunicarea – Internet sau reţeaua locală. Toate acestea pot constitui criterii după care să se realizeze identificarea sursei interceptate, servind modalitatea de apreciere a limitelor admisibilului intervenţiilor în viaţa privată.

Unele aspecte de procedură. În funcţie de procedeul tehnico-tactic ales pentru interceptare, precum şi pentru asigurarea admisibilităţii probei obţinute pe această cale, poate fi necesară o activitate investigativă anterioară pentru determinarea concretă a serviciului prin intermediul căruia acuzatul poartă comunicări ce ar putea interesa procesul penal aflat în desfăşurare. Această ipoteză impune o dublă perspectivă:

1. Dacă demersul procurorului indică expres asupra necesităţii interceptării conversaţiilor purtate prin intermediul unui anume serviciu (Skype, WhatsApp, etc.), judecătorul de instrucţie va fi limitat de solicitarea acestuia şi va putea autoriza preluarea informaţiei transmise în timp real doar în aceste limite. Executarea măsurii respective de investigaţie nu se va putea extinde asupra altor servicii *instant messaging*. Considerentele enunţate permit a aprecia drept oportun un asemenea demers doar în cazul în care urmărirea penală dispune de probe suficiente că acuzatul va purta comunicări importante pentru cauza penală numai printr-un anume serviciu şi probabilitatea că va apela la un altul este nesemnificativă sau neglijabilă.

2. Dacă solicitarea procurorului nu face specificaţie în raport cu tipul mesageriei în timp real care trebuie interceptată, făcând o referire generică la toate convorbirile pe care le poartă subiectul care poate fi supus acestei măsuri speciale de investigaţie, judecătorul de instrucţie va fi îndreptăţit să autorizeze preluarea doar a celor convorbiri în privinţa cărora demersul a argumentat cu referire la materialele cauzei legătura acestora cu una din circumstanţele incluse în obiectul probatoriului, precum şi imposibilitatea obţinerii probei pe altă cale, în condiţiile art.132^1 C.proc. pen. Or, instanţa este însăşi limitată de prevederile normative ale art.132^1 alin.(2) pct.3) C.proc.pen. prin obligativitatea aprecierii, în baza probelor propuse de procuror, nu doar a necesităţii, ci şi a proporţionalităţii restricţiilor drepturilor fundamentale aduse prin aplicarea măsurii respective de investigaţie cu scopul procesului penal în acea cauză.

În egală măsură, cu stabilirea strictă a limitelor domeniului interceptat este necesară aprecierea categoriilor de date care pot fi preluate şi retransmise sau doar citite – doar dialogul/monologul propriuzis sau şi documentele-text, înregistrările audio/video transmise etc., precum şi aprecierea necesităţii unei specificări de acest gen în încheierea instanţei de autorizare a procedeului probatoriu menţionat. Or, prin mesageria instant se pot transmite nu numai date create în procesul comunicării şi rezultate din desfăşurarea dialogului, ci şi documente-text, audio, video etc. anterior create şi remise unuia dintre interlocutori. Fiind o parte a convorbirii realizate ele, de asemenea, pot fi preluate şi, convenţional, incluse în categoria informaţiei interceptate, pentru că deşi nu sunt constituite în momentul comunicării, sunt transmise la momentul realizării acesteia. De aceea, o autorizaţie separată nu este obligatorie, însă o specificare în acest sens în încheierea prin care se admite respectiva acţiune de urmărire penală este necesară. În acest sens, textul legii indică asupra posibilităţii de cunoaştere de către organul de urmărire penală sau ofiţerul de investigaţii a conţinutului comunicării, şi nu doar a formei de prezentare a acesteia.

De regulă, interceptarea comunicărilor, inclusiv a celor electronice, presupune o captare a informaţiilor după tehnici şi procedee similare celor de hack şi, în funcţie de scopul aplicării măsurii respective de investigaţie, poate apela metode active sau pasive de realizare [4, p.4]. Metodele pasive, în principiu, se rezumă doar la o observare a traficului de informaţie, cele active însă presupun modificarea conţinutului de date transmis de sursă punctului de destinaţie, prin excluderea unora dintre ele, inserarea altora noi etc. Interpretarea *ad literam* a textului art. 132^8 alin. (1) C.proc.pen. permite a considera drept admisibilă doar o „citire" a informaţiilor, fără conferirea dreptului subiectului oficial de a opera transformări de orice gen în cuprinsul iniţial al conversaţiilor. În acest sens, folosirea sintagmei „se poate afla conţinutul unor convorbiri" exclude aplicarea unor metode active de interceptare în sensul enunţat. Raţionamentul derivă aici şi din interdicţia provocării, facilitării sau încurajării comiterii infracţiunii sub sancţiunea inadmisibilităţii probei astfel obţinute, potrivit art.94 alin.(1), pct.11) C.proc.pen., care poate fi considerată drept consecinţă cu un grad sporit de probabilitate a intervenirii, întrucât un alt scop al manipulării informaţionale respective nu poate fi constatat. În plus, deoarece acţiunea de urmărire penală menţionată se află sub incidenţa art.8 CEDO, orice limitări aduse inviolabilităţii vieţii private sau secretului corespondenţei trebuie să corespundă le-

gii, iar extinderea competenţelor subiectului oficial în cadrul interceptării, prin oferirea dreptului celui din urmă de a interveni în fondul conversaţiei afectând autenticitatea acesteia, ar putea contraveni cerinţei de previzibilitate [8] care se înaintează actului normativ în acest sens.

În plus, *instant messaging* permite nu numai transferul de date anterior create sau formate în timpul comunicării, ci şi apelul telefonic [9] între două computere sau dispozitive asimilate acestuia [10], de unde şi derivă necesitatea determinării categoriei în care urmează a fi incluse, pentru o apreciere corectă a exigenţelor admisibilităţii legate de administrare. Astfel, atribuirea conversaţiilor respective la grupul celor telefonice propriu-zise sau la al celor electronice, vor face aplicabile criteriile de individualizare a domeniului interceptat şi, implicit, va determina limitele intervenţiilor admisibile în viaţa privată şi secretul corespondenţei.

Din perspectivă tehnică, atunci când aplicaţiile speciale apelează un computer, conexiunea între ele se realizează prin intermediul IP-urilor oferite de punctele de acces la un sistem informatic al mijloacelor tehnice ale ambilor utilizatori. În situaţia apelurilor dintre calculatoare, nu se conectează anumite numere de telefon atribuite abonaţilor de prestatorul serviciilor de telefonie fixă sau mobilă, după regulile telefoniei tradiţionale, ci are loc transferul de date electronice de la un sistem informatic la altul, prin stabilirea unui cod care identifică computerul în cadrul comunicărilor internet de orice gen şi fără de care conexiunea însăşi nu poate avea loc. În acest sens, se vor considera comunicări electronice şi se vor supune cerinţelor de administrare şi admisibilitate ale interceptărilor de acest fel toate apelurile efectuate între două sisteme informatice, dacă acestea se realizează prin intermediul serviciilor *instant messaging* sau celor similare celor din urmă. Drept efect, vor fi considerate electronice şi conversaţiile care au drept mijloc tehnic de realizare telefoanele mobile, în situaţia în care acestea nu se fac în mod direct, apelând centrul de telecomunicaţii ci prin aplicaţiile corespunzătoare, apelând IP-urile atribuite de punctele de acces la reţeaua globală sau locală [11].

Prin urmare, determinarea exactă a limitelor interceptării, prin indicarea aplicaţiilor ce mijlocesc comunicarea, a formelor de comunicare sau a serviciilor prin care se realizează este imperativă, întrucât tot ce depăşeşte limitele autorizate de judecătorul de instrucţie vor constitui date ce nu vor putea fi admise ca probă, iar un mandat prea larg nu este, în principiu, acceptabil [5]. În funcţie de natura infracţiunii cercetate, de materialul probant existent în cauză, de prezenţa criteriului de urgenţă şi alte circumstanţe particulare ale cauzei, unul sau mai multe criterii pot fi apreciate ca suficiente de judecătorul de instrucţie pentru a aprecia proporţionalitatea intervenţiei şi admiterea măsurii.

Referințe:

1. *Recomandarea nr. R(95)13 a Comitetului de Miniştri către statele membre cu privire la problemele de procedură penală legate de tehnologiile informaţionale,* adoptată la 11 septembrie 1995, în cadrul celei de-a 543-a reuniuni a Delegaţilor Miniştrilor.

2. *Convenţia europeană privind criminalitatea informatică,* adoptată la Budapesta la 23 noiembrie 2001.

3. United States Code of the Federal Government of the United States, 18 USC §2510, http://www.law.cornell.edu/uscode/text (accesat: 05.03.17).

4. Dobrinoiu M. *Interceptarea ilegală a unei transmisii de date informatice.* Disponibil la: http://e-crime.ro/ecrime/site/files/57341236022318interceptareadatelorinformaticeCHIP.pdf (accesat: 05.03.17).\

5. Curtea Europeană a Drepturilor Omului, *cauza Robathin v. Austria*, 03.10.2012.

6. În acest sens, în tehnică se operează cu termenul de *instant messaging (IM)* sau *chat*, utilizat pentru a defini comunicarea, prin intermediul programelor speciale, realizată imediat/în timp real între doi sau mai mulţi utilizatori aflaţi, de regulă, în regim online. Excepţia se referă la reţeaua locală care oferă posibilitatea apelării mesageriei instant chiar şi în regim offline.

7. Grossman Andrew M.*, No, don't IM me--instant messaging, authentication, and the best evidence rule*, George Manson Law Review, 2006. Disponibil la: http://georgemasonlawreview.org/wp-content/uploads/2014/03/13-6_Grossman.pdf (accesat: 05.03.2017).

8. Curtea Europeană a Drepturilor Omului, *cauza Rotaru v. România*, 04.05.2000; Curtea Europeană a Drepturilor Omului, *cauza Liberty ş.a. v. Regatul Unit* 01.07.2008.

9. Aplicaţiile de tipul WhatsApp şi Skype oferă posibilitatea utilizatorilor de a efectua apeluri telefonice audio sau audiovideo, asigurând conexiunea între două sisteme informatice aflate în reţea.

10. Prin dispozitive asimilate în acest context se înţelege orice sistem informatic care prin intermediul unor programe speciale poate realiza comunicarea de date (de ex. telefonul mobil, tableta, etc.).

11. În internet apelurile se realizează prin intermediul serviciului VOIP (un tip de telefonie bazată pe transmiterea semnalului vocal de la un sistem informatic la altul) în cadrul căruia identificarea interlocutorilor este făcută prin intermediul adresei IP.