



MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 189 (XXXIII) — Nr. 171

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Vineri, 19 februarie 2021

SUMAR

<u>Nr.</u>	<u>Pagina</u>
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE	
24. — Ordin al ministrului afacerilor interne pentru completarea Metodologiei privind elaborarea normelor și tabelelor de înzestrare cu armament, muniții, mijloace tehnice și materiale necesare structurilor Ministerului Afacerilor Interne, aprobată prin Ordinul ministrului afacerilor interne nr. 28/2018	2
6.457. — Ordin al șefului Departamentului pentru Situații de Urgență privind instituirea măsurii de carantină zonală pentru comuna Groși, cu satele aparținătoare Groși, Ocoliş și Satu Nou de Jos, județul Maramureș	2–4
ACTE ALE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE	
Decizia nr. 4 din 25 ianuarie 2021 (Completul pentru dezlegarea unor chestiuni de drept în materie penală)	5–16

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL AFACERILOR INTERNE

ORDIN

**pentru completarea Metodologiei privind elaborarea normelor
și tabelelor de înzestrare cu armament, muniții, mijloace
tehnice și materiale necesare structurilor Ministerului
Afacerilor Interne, aprobată prin Ordinul ministrului
afacerilor interne nr. 28/2018**

În temeiul art. 7 alin. (5) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare,

ministrul afacerilor interne emite următorul ordin:

Art. I. — După articolul 3 din Metodologia privind elaborarea normelor și tabelelor de înzestrare cu armament, muniții, mijloace tehnice și materiale necesare structurilor Ministerului Afacerilor Interne, aprobată prin Ordinul ministrului afacerilor interne nr. 28/2018, publicat în Monitorul Oficial al României, Partea I, nr. 293 din 2 aprilie 2018, se introduce un nou articol, articolul 3¹, cu următorul cuprins:

„Art. 3¹. — Prin excepție de la prevederile art. 3, bunurile materiale necesare structurilor M.A.I. pentru activitățile desfășurate în vederea asigurării managementului proiectelor/programelor finanțate din fonduri externe nu se înscriu în normele și tablele de înzestrare.”

Art. II. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

p. Ministrul afacerilor interne,
Bogdan Despescu,
secretar de stat

București, 11 februarie 2021.
Nr. 24.

MINISTERUL AFACERILOR INTERNE
DEPARTAMENTUL PENTRU SITUAȚII DE URGENȚĂ

ORDIN

**privind instituirea măsurii de carantină zonală pentru comuna Groși,
cu satele aparținătoare Groși, Ocoliș și Satu Nou de Jos, județul Maramureș**

Luând în considerare situația epidemiologică la nivelul comunei Groși, cu satele aparținătoare Groși, Ocoliș și Satu Nou de Jos, județul Maramureș, generată de coronavirusul SARS-CoV-2, având ca rezultat o incidență a cazurilor de îmbolnăvire cu SARS-CoV-2 de 6,32 cazuri la 1.000 de locuitori, riscul epidemiologic fiind de o gravitate maximă, în circumstanțe de nerespectare a măsurilor legale în vigoare,

ținând cont de Hotărârea Comitetului Județean pentru Situații de Urgență Maramureș nr. 20/2021 din 18.02.2021 emisă pe baza Analizei de risc a Direcției de Sănătate Publică a Județului Maramureș nr. 4.373 din 18.02.2021 și a Avizului Institutului Național de Sănătate Publică nr. 2.702/18.02.2021,

în temeiul prevederilor art. 3 lit. b), art. 6 lit. b), art. 7 alin. (5) și art. 12 alin. (1) din Legea nr. 136/2020 privind instituirea unor măsuri în domeniul sănătății publice în situații de risc epidemiologic și biologic, ale art. 5 alin. (3) lit. a)—d) și f) din Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare, ale art. 11 alin. (3) din Hotărârea Guvernului nr. 557/2016 privind managementul tipurilor de risc, ale art. 3 din Hotărârea Guvernului nr. 35/2021 privind prelungirea stării de alertă pe teritoriul României începând cu data de 12 februarie 2021, precum și stabilirea măsurilor care se aplică pe durata acesteia pentru prevenirea și combaterea efectelor pandemiei de COVID-19 și ale art. 3 alin. (4) din Ordinul nr. 1.309/2020 privind modalitatea de aplicare a măsurilor de prevenire și limitare a îmbolnăvirilor cu SARS-CoV-2,

șeful Departamentului pentru Situații de Urgență emite următorul ordin:

Art. 1. — (1) Se instituie măsura de carantină zonală, începând cu data de 19.02.2021, ora 8,00, pentru o perioadă de 14 zile, până în data de 5.03.2021, ora 8,00, pentru comuna Groși, cu satele aparținătoare Groși, Ocoliș și Satu Nou de Jos, județul Maramureș.

(2) Perimetrul vizat de măsura prevăzută la alin. (1) este delimitat de limita administrativă a unității administrativ-teritoriale cuprinsă între următoarele coordonate geografice:
Latitudine: 47.62558 N, Longitudine: 23.5479
Latitudine: 47.60927 N, Longitudine: 23.55124 E

Latitudine: 47.5934 N, Longitudine: 23.5796 E
Latitudine: 47.61515 N, Longitudine: 23.6268 E
Latitudine: 47.62898 N, Longitudine: 23.61049 E.

Art. 2. — Este strict interzisă intrarea/ieșirea în/din zona carantinată prin alte zone și căi de acces decât cele deschise circulației publice de pe drumurile naționale, județene, comunale și forestiere.

Art. 3. — Circulația și staționarea în spații publice a persoanelor sunt interzise, cu excepția motivelor bine justificate, pe baza declarației pe propria răspundere, legitimației de serviciu sau a adevărâței eliberate de angajator.

Art. 4. — Se instituie următoarele măsuri obligatorii pentru toate persoanele care se află permanent sau tranzitează zona carantinată:

1. identificarea tuturor persoanelor cu domiciliul, reședința ori adresa declarată în zona menționată la art. 1 alin. (2) și introducerea acestora în bazele de date dedicate;

2. limitarea la maximum a deplasării persoanelor și monitorizarea permanentă a respectării acestei măsuri. Ieșirea persoanelor din locuință este permisă doar pe bază de declarație pe proprie răspundere, legitimație de serviciu sau adevărâță eliberată de angajator, după caz;

3. în intervalul orar 6,00—22,00, în interiorul zonei menționate la art. 1 alin. (2) se interzice circulația tuturor persoanelor în afara locuinței/gospodăriei, cu următoarele excepții:

a) deplasarea în interes profesional, inclusiv între locuință/gospodărie și locul/locurile de desfășurare a activității profesionale și înapoi;

b) deplasarea pentru asigurarea de bunuri care acoperă necesitățile de bază ale persoanelor, precum și bunuri necesare desfășurării activității profesionale;

c) deplasarea pentru asistență medicală care nu poate fi amânată și nici realizată de la distanță;

d) deplasările scurte, în apropierea locuinței/gospodăriei, legate de activitatea fizică individuală a persoanelor (cu excluderea oricăror activități sportive de echipă), precum și pentru nevoile animalelor de companie/domestice;

e) deplasarea în scopul donării de sânge/plasmă la centrele de transfuzie sanguină;

f) deplasarea în scop umanitar sau de voluntariat;

g) deplasarea pentru realizarea de activități agricole;

h) deplasarea producătorilor agricoli pentru comercializarea de produse agroalimentare;

i) îngrijirea sau administrarea unei proprietăți din altă localitate;

j) participarea la programe sau proceduri în centrele de tratament;

k) pentru achiziția, service-ul, efectuarea ITP sau alte operațiuni de întreținere a vehiculelor, activități care nu pot fi efectuate în localitatea de domiciliu;

l) eliberarea de documente necesare pentru obținerea unor drepturi prevăzute de lege;

m) alte motive justificate, precum: îngrijirea/însoțirea copiilor/membrilor de familie, îngrijirea unei/unui rude/afin sau persoane aflate în întreținere, asistența persoanelor vârstnice, bolnave sau cu dizabilități ori decesul unui membru de familie;

n) participarea la activități religioase;

o) deplasări ale persoanelor care sunt în tranzit sau efectuează călătorii al căror interval se suprapune cu perioada interdicției, cum ar fi cele efectuate cu trenul, avionul, autocarul sau alte mijloace de transport persoane și care poate fi dovedit prin bilet sau oricare altă modalitate de achitare a datoriei;

p) deplasări ale persoanelor pentru administrare de vaccin împotriva SARS-CoV-2;

4. în intervalul orar 22,00—6,00, circulația persoanelor în afara locuinței/gospodăriei este permisă numai pentru motivele prevăzute la pct. 3 lit. a), c), m) și o);

5. în/din zona menționată la art. 1 alin. (2) este permisă intrarea/ieșirea pentru:

a) transportul de marfă, indiferent de natura acestuia, al materiilor prime și resurselor necesare desfășurării activităților economice în localitatea carantinată, precum și aprovizionarea populației;

b) persoanele care nu locuiesc în zona carantinată, dar care desfășoară activități economice sau în domeniul apărării, ordinii publice, securității naționale, sanitar, veterinar, situațiilor de urgență, administrației publice locale, asistenței și protecției sociale, judiciar, serviciilor de utilitate publică, agriculturii, alimentației publice, comunicațiilor și transporturilor;

c) persoanele care locuiesc în zona carantinată și desfășoară activitatea profesională în afara zonei carantinate;

d) persoanele care realizează activități agricole sau pentru comercializarea de produse agroalimentare;

e) deplasarea din alte motive justificate, precum îngrijirea/însoțirea copiilor/membrilor de familie, îngrijirea unei/unui rude/afin sau a unei persoane aflate în întreținere, asistența persoanelor vârstnice, bolnave sau cu dizabilități, decesul unui membru de familie;

f) deplasarea pentru asistență medicală care nu poate fi amânată și nici realizată de la distanță;

g) urgențe medicale;

6. pentru verificarea motivului deplasării în interes profesional, persoanele sunt obligate să prezinte, la cererea personalului autorităților abilitate, legitimația de serviciu, adevărâța eliberată de angajator sau o declarație pe propria răspundere;

7. pentru verificarea motivului deplasării în interes personal, persoanele sunt obligate să prezinte, la cererea personalului autorităților abilitate, o declarație pe propria răspundere, completată în prealabil;

8. declarația pe propria răspundere trebuie să cuprindă numele și prenumele, data nașterii, adresa locuinței/gospodăriei/locului activității profesionale, motivul deplasării conform celor prevăzute la art. 4 pct. 3 și 5, data completării și semnătura;

9. se permite tranzitarea comunei Groși, cu satele aparținătoare Groși, Ocoliş și Satu Nou de Jos, de către persoanele care nu au domiciliul pe raza acesteia, fiind interzisă oprirea în localitățile carantinate zonal;

10. prin grija administrației publice locale și a Inspectoratului de Poliție al Județului Maramureș se vor stabili căile de circulație pentru tranzitarea zonei respective și aducerea la cunoștința populației prin mass-media a acestei măsuri;

11. prin activitățile religioase de la art. 4 lit. n) se înțeleg următoarele:

a) slujbele religioase cu caracter colectiv se pot oficia în lăcașurile de cult, fără accesul publicului, putând fi transmise prin mass-media sau online;

b) slujbele religioase cu caracter privat (botezuri, cununii, înmormântări) se pot oficia în lăcașurile de cult, cu participarea a maximum 16 persoane (număr ce include și persoanele care oficiază slujba religioasă);

c) este permis accesul credincioșilor în lăcașurile de cult pentru rugăciuni cu caracter individual, astfel încât să fie asigurată o suprafață de minimum 4 mp pentru fiecare persoană și o distanță de minimum 2 m între persoane;

d) slujbele religioase care se vor oficia în aer liber se vor desfășura cu menținerea distanței de 1,5 m între persoane;

12. la toate slujbele religioase trebuie respectate regulile de protecție sanitară stabilite prin ordinul comun al ministrului sănătății și al ministrului afacerilor interne, cu avizul secretarului de stat pentru culte, emis în temeiul art. 45 și al art. 71 alin. (2) din Legea nr. 55/2020, cu modificările și completările ulterioare;

13. controlul măsurilor privind limitarea deplasării persoanelor în/din comuna Groși, cu satele aparținătoare Groși, Ocoliş și Satu Nou de Jos, județul Maramureș, și asigurarea ordinii publice se vor realiza de către Inspectoratul de Jandarmi Județean Maramureș sau Inspectoratul de Poliție al Județului Maramureș, după caz.

Art. 5. — În zona prevăzută la art. 1 alin. (2) se interzic următoarele activități:

1. organizarea de evenimente private (nunți, botezuri, mese festive etc.) în spații închise și deschise;

2. organizarea de evenimente și/sau activități private pentru copii în spații închise cum ar fi evenimente aniversare, locuri de joacă, spații de tip after-school etc.;

3. activitatea cu publicul a operatorilor economici care desfășoară activități de preparare, comercializare și consum al produselor alimentare și/sau băuturilor alcoolice și nealcoolice, de tipul restaurantelor și cafenelelor, inclusiv al teraselor, în interiorul și exteriorul clădirilor (se pot comercializa produse alimentare în regim catering — livrare la domiciliu);

4. activitatea cu publicul a operatorilor economici licențiați în domeniul jocurilor de noroc, indiferent de locațiile amplasate, cu excepția celor care comercializează bilete de tip LOTO, pariuri și lozuri, conform Adresei INSP nr. 19.941/2020 și a Hotărârii CNSU nr. 60/2020;

5. activitatea cu publicul a structurilor de primire turistică, cu excepția cazării persoanelor care efectuează deplasări în interes profesional;

6. organizarea și desfășurarea activităților de tipul spectacolelor și/sau concertelor;

7. organizarea și desfășurarea activităților culturale, științifice, artistice sau de divertisment, în spații închise sau deschise;

8. toate activitățile și competițiile sportive, individuale sau colective, care se desfășoară în spații închise sau deschise, cu excepția celor profesioniste organizate de federațiile de profil.

Art. 6. — (1) Se limitează programul de lucru cu publicul al operatorilor economici din domeniul comercializării de bunuri alimentare și nealimentare până la ora 21,00, cu excepția farmaciilor și a stațiilor de distribuție carburant, care pot avea program non-stop și în care personalul de serviciu va deservi clienții la geam.

(2) Se limitează numărul de persoane în incinta magazinelor, cu respectarea normelor de distanțare fizică, cu asigurarea pentru clienți a unei suprafețe de 4 mp (din suprafața utilă a magazinului) și cu păstrarea distanței de 2 m între persoane.

Art. 7. — Operatorii economici care desfășoară activități de transport persoane și care tranzitează zonă carantinată vor putea efectua opriri/porniri doar în stații pentru urcarea sau coborârea călătorilor. Activitatea acestora se va desfășura prin ocuparea a 50% din locurile existente pe scaun în fiecare vehicul și cu respectarea normelor de protecție sanitară stabilite în perioada stării de alertă pentru prevenirea răspândirii SARS-CoV-2, în următoarele condiții:

— administratorii vor dezinfecta mijloacele de transport după fiecare cursă efectuată;

— pasagerii vor purta masca de protecție pe tot parcursul călătoriei;

— numărul de pasageri permis în fiecare mijloc de transport va fi egal cu jumătate din numărul locurilor de pe scaun existente în fiecare mijloc de transport;

— se va respecta circuitul de urcare/coborâre în mijlocul de transport. Accesul pasagerilor se va realiza pe ușa din față, iar coborârea pe ușa din spate.

Art. 8. — Măsurile stabilite potrivit prevederilor prezentului ordin vor fi comunicate autorităților publice locale și vor fi aduse la cunoștința populației prin utilizarea sistemului RO-ALERT, precum și prin alte mijloace.

Art. 9. — În conformitate cu prevederile Hotărârii CNSU nr. 5/2021 și Ordinului comun ME și MS nr. 3.235/93/2021,

cursurile de învățământ se vor desfășura în comuna Groși, cu satele aparținătoare Groși, Ocoliş și Satu Nou de Jos, doar în sistem online.

Art. 10. — Direcția de Sănătate Publică Maramureș va întreprinde următoarele:

(1) analizarea oportunităților și prioritizarea testării persoanelor, transmiterea solicitărilor de sprijin cu materiale sanitare și personal de specialitate către Institutul Național de Sănătate Publică/Ministerul Sănătății;

(2) stabilirea unui calendar periodic pentru dezinfectarea spațiilor publice, la un interval de 48 de ore, și urmărirea îndeplinirii acestuia de către unitatea administrativ-teritorială în cauză;

(3) îndrumarea și implicarea medicilor de familie de pe raza localității în monitorizarea din punct de vedere medical a persoanelor izolate/carantinate la domiciliu și acordarea asistenței medicale a populației din zona respectivă (femei gravide, persoane în program de hemodializă, pacienți oncologici etc.);

(4) supravegherea colectării deșeurilor medicale în cadrul contractual cu cabinetele medicilor de familie și asigurarea respectării normelor specifice acestei activități.

Art. 11. — Inspectoratul pentru Situații de Urgență „Basarab I” al Județului Maramureș asigură transmiterea mesajelor de avertizare prin sistemul RO-ALERT către populația din comuna Groși, cu satele aparținătoare Groși, Ocoliş și Satu Nou de Jos, cu măsurile ce trebuie respectate pe timpul instituirii carantinei.

Art. 12. — (1) Nerespectarea măsurilor prevăzute de prezentul ordin atrage răspunderea disciplinară, civilă, contravențională sau penală, în conformitate cu prevederile art. 64 din Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare.

(2) Sunt abilitate să verifice respectarea măsurilor de mai sus categoriile de personal prevăzute de art. 67 din Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare.

Art. 13. — Alte măsuri pentru prevenirea și combaterea răspândirii SARS-CoV-2, precum și pentru soluționarea unor probleme deosebite pe perioada carantinei vor fi stabilite prin Centrul Județean de Coordonare și Conducere a Intervenției Maramureș (telefon 0262.212.209, e-mail: cjcci@isumm.ro).

Art. 14. — Prezentul ordin se va transmite spre aplicare la Centrul Județean de Coordonare și Conducere a Intervenției Maramureș, care va asigura informarea președintelui Comitetului Județean pentru Situații de Urgență Maramureș și a Direcției de Sănătate Publică Maramureș, și spre informare la Institutul Național de Sănătate Publică, Ministerul Sănătății — Direcția generală de asistență medicală, medicină de urgență și programe de sănătate publică, Inspectoratul General al Poliției Române și Inspectoratul General al Jandarmeriei Române.

Art. 15. — Prevederile prezentului ordin au aplicabilitate din data de 19.02.2021, ora 8,00, pentru o perioadă de 14 zile, până în data de 5.03.2021, ora 8,00, măsurile stabilite în aplicarea acestui ordin urmând a fi raportate până în data de 19.02.2021, ora 18,00, la Centrul Național de Coordonare și Conducere a Intervenției.

Art. 16. — Prezentul ordin se transmite pentru publicare pe site-urile oficiale ale Ministerului Afacerilor Interne, Departamentului pentru Situații de Urgență și Inspectoratului General pentru Situații de Urgență.

Art. 17. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Șeful Departamentului pentru Situații de Urgență,

Raed Arafat,
secretar de stat

ACTE ALE ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE

COMPLETUL PENTRU DEZLEGAREA UNOR CHESTIUNI DE DREPT ÎN MATERIE PENALĂ

DECIZIA Nr. 4**din 25 ianuarie 2021**

Dosar nr. 2.534/1/2020

Daniel Grădinaru — președintele Secției penale a Înaltei Curți de Casație și Justiție — președintele completului
 Andrei Claudiu Rus — judecător la Secția penală
 Alin Sorin Nicolescu — judecător la Secția penală
 Dan Andrei Enescu — judecător la Secția penală
 Lucia Tatiana Rog — judecător la Secția penală
 Francisca Maria Vasile — judecător la Secția penală
 Ionuț Mihai Matei — judecător la Secția penală
 Constantin Epure — judecător la Secția penală
 Valentin Horia Șelaru — judecător la Secția penală

Pe rol pronunțarea asupra sesizării formulate de Curtea de Apel Brașov — Secția penală în Dosarul nr. 9.010/197/2019 privind dezlegarea următoarei chestiuni de drept: „*Dacă fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului.*”

Dezbaterile au avut loc în ședința din data de 20 ianuarie 2021, fiind consemnate în încheierea de ședință de la aceeași dată, care face parte integrantă din prezenta decizie, când Înalta Curte de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept în materie penală, având nevoie de timp pentru a delibera, a stabilit termen pentru pronunțare la data de 25 ianuarie 2021, când, în aceeași compunere, a decis următoarele:

ÎNALTA CURTE,

asupra chestiunii de drept cu care a fost sesizată, constată următoarele:

I. Titularul și obiectul sesizării

Prin Încheierea de ședință din data de 2 septembrie 2020 pronunțată în Dosarul nr. 9.010/197/2019, Curtea de Apel Brașov — Secția penală a dispus sesizarea Înaltei Curți de Casație și Justiție în vederea dezlegării următoarei chestiuni de drept: „*Dacă fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului.*”

II. Expunerea succintă a cauzei

Curtea de Apel Brașov — Secția penală a fost sesizată cu apelul declarat de inculpatul D.M. împotriva Sentinței penale

nr. 478 din data de 2 aprilie 2020 pronunțate de Judecătoria Brașov.

În cauză, prin Rechizitoriul nr. 11.255/P/2018 din data de 1 aprilie 2019 al Parchetului de pe lângă Judecătoria Brașov s-a dispus trimiterea în judecată, în stare de libertate, a inculpatului D.M. sub aspectul săvârșirii infracțiunilor de *șantaj*, prevăzută de art. 207 alin. (1) și (2) din Codul penal, *violarea vieții private în formă continuată*, prevăzută de art. 226 alin. (2) din Codul penal cu aplicarea art. 35 alin. (1) din Codul penal (două acte materiale) și *fals informatic în formă continuată*, prevăzută de art. 325 din Codul penal cu aplicarea art. 35 alin. (1) din Codul penal (două acte materiale), toate cu aplicarea art. 38 alin. (1) din Codul penal.

În sarcina inculpatului s-au reținut, în esență, următoarele fapte:

— în cursul lunii decembrie 2018, inculpatul a amenințat-o, în repetate rânduri, pe persoana vătămată B.P.A., prin intermediul telefonului și a rețelelor de socializare, că va da publicității pe internet mai multe fotografii, care o înfățișau dezbrăcată și filmulețe, care o înfățișau pe aceasta întreținând relații sexuale normale cu el, dacă nu va accepta să întrețină în continuare relații sexuale cu inculpatul, deși persoana vătămată nu mai dorea acest lucru, reținându-se că fapta întrunește elementele constitutive ale infracțiunii de șantaj, prevăzută de art. 207 alin. (1) și (2) din Codul penal;

— în cursul lunii decembrie 2018, inculpatul a creat pe site-ul www.pornhub.com un profil cu numele persoanei vătămate B.P.A., pe care a postat mai multe fotografii cu persoana vătămată nud și un filmuleț în care persoana vătămată întreținea relații sexuale cu el (primul act material) și a creat un profil fals pe rețeaua de socializare Facebook cu numele persoanei vătămate B.P.A., de pe care i-a trimis martorului D.S. mai multe fotografii cu persoana vătămată dezbrăcată (al doilea act material), în ipostaze intime, reținându-se că faptele întrunesc elementele constitutive ale infracțiunilor de fals informatic în formă continuată, prevăzută de art. 325 din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal, și violarea vieții private, prevăzută de art. 226 alin. (2) din Codul penal, cu aplicarea art. 35 alin. (1) din Codul penal.

Prin Sentința penală nr. 478 din data de 2 aprilie 2020 a Judecătoriei Brașov s-a dispus condamnarea inculpatului pentru toate infracțiunile imputate, apreciindu-se dovedită starea de fapt descrisă prin rechizitoriu, în drept fiind reținută aceeași încadrare ca cea dată infracțiunilor în cursul urmăririi penale.

Cu referire la realizarea conținutului constitutiv al infracțiunii de fals informatic, instanța de fond a arătat că, potrivit dispozițiilor art. 325 din Codul penal, constituie infracțiunea de fals informatic *fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice.*

Pentru realizarea laturii obiective a acestei infracțiuni este necesar ca agentul să interacționeze cu datele informatice stocate într-un *sistem informatic* ori într-un *mediu de stocare* în

asa fel încât să rezulte date necorespunzătoare adevărului, iar scopul agentului să fie acela de a utiliza aceste date în vederea producerii unor consecințe juridice. Aceste două elemente indică un paralelism evident cu falsul tradițional în înscrisuri. Modalitatea în care a acționat inculpatul D.M. este cea a *introducerii de date informatice*, ceea ce reprezintă corespondentul acțiunii de contrafacere a unui înscris. Astfel, se reține introducerea de date informatice atunci când autorul creează un document electronic fals. S-a reținut că doctrina și jurisprudența sunt unanim de acord că *inclusiv crearea unui profil fals în cadrul unei rețele de socializare, prin utilizarea datelor de identificare ale unei persoane*, poate realiza tipicitatea textului de incriminare.

Acțiunile inculpatului de a crea un profil fals pe contul de socializare Facebook cu numele persoanei vătămate, precum și pe site-ul www.pornhub.com un profil cu numele persoanei vătămate B.P.A. au avut ca scop prestabilit denigrarea publică și defăimarea imaginii acesteia la serviciu și în cercul de prieteni.

Sub aspectul *laturii subiective*, s-a reținut că atitudinea psihică a inculpatului față de fapte și de urmările acestora îmbracă forma vinovăției în modalitatea intenției directe, conform art. 16 alin. (3) lit. a) din Codul penal, deoarece inculpatul a prevăzut și urmărit rezultatul faptelor sale (atingerea relațiilor sociale referitoare la libertatea psihică a persoanei vătămate, viața privată a acesteia și dreptul persoanei la propria imagine), acesta exercitând amenințări la adresa persoanei vătămate în scopul obținerii de favoruri sexuale, furându-i identitatea în scopul creării unor profile false pe rețelele de socializare, în vederea discreditării și ponegririi în public a acesteia.

Împotriva Sentinței penale nr. 478 din data de 2 aprilie 2020 pronunțate de Judecătoria Brașov — Secția penală a formulat apel inculpatul D.M., în cuprinsul motivelor de apel invocând, printre altele, netemeinicia soluției de condamnare pentru săvârșirea infracțiunii de fals informatic, susținând că nu sunt realizate cerințele esențiale ale acestei infracțiuni.

În faza de apel, la termenul de judecată din data de 14 iulie 2020, instanța, din oficiu, a pus în discuția părților necesitatea sesizării Înaltei Curți de Casație și Justiție în vederea pronunțării unei hotărâri prealabile pentru dezlegarea unei chestiuni de drept, în condițiile art. 475 și următoarele din Codul de procedură penală.

În acest sens, instanța a constatat că, în cauză, urmează să analizeze, printre altele, dacă crearea unui cont pe o rețea de socializare accesibilă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată **fără drept** și, respectiv, să aibă ca rezultat **date necorespunzătoare adevărului**, chestiune de drept, în condițiile în care presupune încadrarea în condițiile de tipicitate prevăzute de art. 325 din Codul penal a unei anumite situații de fapt.

În ceea ce privește utilitatea unei interpretări unitare oferite de Înalta Curte de Casație și Justiție, s-a arătat că în practica recentă a Curții de Apel Brașov au existat mai multe dosare în care, în situații de fapt similare celei deduse judecării în prezenta cauză, s-a dispus trimiterea în judecată a inculpatului pentru săvârșirea infracțiunii de fals informatic în concurs cu violarea vieții private.

Soluțiile în aceste cauze au fost diferite, variind de la condamnare (astfel cum s-a întâmplat în prezenta cauză, în primă instanță), achitare (soluție dispusă în primă instanță și menținută în apel — în acest sens fiind Dosarul nr. 9.754/

197/2019 al Judecătoria Brașov — Secția penală) sau schimbarea încadrării juridice din cele două infracțiuni menționate anterior, în concurs, în infracțiunea unică de violare a vieții private (în acest sens fiind soluția dispusă în Dosarul nr. 31.106/197/2018 al Curții de Apel Brașov — Secția penală).

În toate aceste cauze s-a pus în discuție realizarea conținutului constitutiv al infracțiunii de fals informatic.

Sub aspectul admisibilității sesizării, instanța de apel a considerat că sunt îndeplinite condițiile prevăzute de art. 475 din Codul de procedură penală, respectiv: cauza se află pe rolul Curții de Apel Brașov, investită cu soluționarea cauzei în ultimă instanță; există o chestiune de drept, de a cărei lămurire depinde soluționarea pe fond a cauzei; asupra acestei chestiuni Înalta Curte de Casație și Justiție nu a statuat anterior printr-o hotărâre prealabilă sau printr-un recurs în interesul legii și, conform verificărilor efectuate, nu există un recurs în interesul legii în curs de soluționare având același obiect.

Punctele de vedere ale Ministerului Public și inculpatului

Reprezentantul Parchetului de pe lângă Curtea de Apel Brașov a apreciat că sunt îndeplinite condițiile de admisibilitate a sesizării Înaltei Curți de Casație și Justiție și a arătat că, ținând cont de modalitatea diferită în care ar putea fi interpretate dispozițiile art. 325 din Codul penal, este util să fie obținută o interpretare a chestiunii de drept invocate, de a cărei lămurire depinde soluționarea pe fond a cauzei.

Apărătorul ales al inculpatului a susținut că sunt îndeplinite condițiile prevăzute de art. 475 din Codul de procedură penală, iar pe fondul chestiunii de drept supuse analizei a arătat că își menține opinia exprimată în cuprinsul motivelor de apel, în sensul că nu sunt realizate condițiile de tipicitate ale infracțiunii de fals informatic.

Punctul de vedere al instanței

Curtea de Apel Brașov — Secția penală a reținut că infracțiunea de fals informatic presupune ca săvârșirea uneia dintre acțiunile prevăzute alternativ de art. 325 din Codul penal (introducere, modificare, ștergere date informatice sau restricționarea accesului la acestea) să fie realizată *fără drept* și să aibă ca rezultat crearea unor *date necorespunzătoare adevărului*.

În opinia instanței, noțiunea de *fără drept* trebuie analizată prin prisma dispozițiilor art. 35 alin. (2) din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, în conformitate cu care *acționează fără drept persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic*.

În acest sens, s-a avut în vedere faptul că infracțiunea de fals informatic a fost inițial incriminată prin dispozițiile art. 48 din Legea nr. 161/2003, tipicitatea faptei rămânând neschimbată și după modificarea sediului legislativ al infracțiunii (existând doar o reducere a limitelor de pedeapsă). De asemenea, noțiunile de *sistem informatic și date informatice*, definite în prezent prin art. 181 din Codul penal, se regăsesc, aproape identic, în art. 35 alin. (1) din Legea nr. 161/2003. În acest context, după cum s-a arătat și în doctrină (spre exemplu, G. Bodoroncea, V. Cioclei ș.a., *Codul penal. Comentariu pe articole*, Ed. C. H. Beck, Ediția 2, 2016), noțiunea „fără drept” din cuprinsul art. 325 din Codul penal este definită de art. 35 alin. (2) din Legea nr. 161/2003.

Or, în opinia instanței, din aceste texte de lege rezultă că *autorizarea sau permisiunea* sunt legate de folosirea sistemului

informatic și *persoana fizică sau juridică competentă* să le acorde este deținătoarea drepturilor asupra sistemului informatic sau datelor informatice.

În cazul unor rețele de tipul celor utilizate de inculpat în cauză — facebook, pornhub — drepturile asupra contului, incluzând toate datele asociate acestuia, aparțin, pe de o parte, deținătorului aplicației (care păstrează anumite drepturi asupra acestuia — spre exemplu, poate elimina anumite date în măsura în care contravin politicii rețelei) și, pe de altă parte, deținătorului (titularului) contului.

Cu privire la această ultimă chestiune, instanța a apreciat relevant și faptul că rețelele amintite nu condiționează deschiderea unui cont de folosirea numelui real al persoanei care utilizează contul și nu efectuează verificări menite a stabili identitatea dintre numele persoanei care deschide contul și numele sub care este înregistrat contul. De altfel, este de notorietate, cel puțin printre utilizatorii unor astfel de rețele, că în cele mai multe dintre cazuri nu sunt folosite numele reale. Este, de asemenea, de necontestat că dreptul de administrare a contului aparține persoanei care l-a deschis (și care se identifică cu datele solicitate de aplicație — nume de utilizator, parolă, număr de telefon etc.), și nu persoanei al cărei nume a fost folosit ca denumire a contului.

În raport cu cele expuse, instanța a considerat, în interpretarea noțiunii de *fără drept*, că aceasta nu trebuie legată de persoana vătămată și de necesitatea ca aceasta să îi permită inculpatului să introducă, în sistemul informatic, date privind persoana sa (fotografii, filme). Nu este vorba de un drept asupra unor astfel de reprezentări ale realității, ci de dreptul de a utiliza sistemul informatic și programul informatic aferent rețelei de socializare.

Pe cale de consecință, dacă o persoană este titularul contului (inclusiv în situația în care a folosit, pentru denumirea acestuia, un nume aparținând altei persoane), aceasta este persoana care are dreptul de a folosi contul respectiv (prin introducerea oricăror date informatice, modificarea acestora, ștergerea etc.), neputându-se reține că a acționat *fără drept*.

În ceea ce privește cea de-a doua condiție supusă discuției, respectiv ca acțiunea de introducere de date informatice să aibă ca rezultat *date necorespunzătoare adevărului*, instanța a considerat că trebuie lămurit aspectul dacă folosirea numelui unei alte persoane pentru deschiderea unui cont într-o rețea de natura celei utilizate de inculpat în cauză (facebook, pornhub) conduce la un astfel de rezultat.

În concret, instanța a avut în vedere situația în care postările inculpatului conțin imagini (fotografii și imagini video) care înfățișează persoana vătămată, imagini reale (neprocedându-se la alterarea lor în nicio formă), astfel că singura împrejurare care nu are corespondent în realitate este faptul că persoana vătămată, al cărei nume apare la denumirea contului, este chiar deținătoarea acestui cont.

Or, în această situație, instanța a considerat că numele persoanei vătămate, regăsit ca nume al contului, nu reprezintă *date informatice necorespunzătoare adevărului*, ceea ce nu corespunde realității fiind situația de fapt rezultând din crearea contului sub un alt nume. Astfel, se ajunge în situația în care titularul contului se prezintă celorlalți utilizatori ai aplicației sub o altă identitate, cea regăsită în denumirea contului. S-a făcut trimitere la dispozițiile art. 327 din Codul penal, care incriminează fapta de fals privind identitatea doar în situația în care este realizată în raport cu o *persoană dintre cele prevăzute în art. 175 sau este transmisă unei unități în care aceasta își desfășoară activitatea*, simpla prezentare sub o identitate falsă altor subiecți de drept nefiind incriminată. Or, în condițiile în care, în realitatea obiectivă, nu este sancționată o astfel de faptă, s-a apreciat că apare ca nefiind justificată o interpretare care să sancționeze o astfel de conduită în *realitatea virtuală*.

În ceea ce privește o eventuală asemănare cu infracțiunea de fals în înscrisuri, rezultând din inserarea numelui unei alte persoane, instanța a apreciat că trebuie să se aibă în vedere faptul că, astfel cum s-a arătat anterior, acest tip de rețele nu garantează existența unei identități între numele de utilizator și numele real al persoanei care deține contul, astfel că simpla introducere a unui nume nu este de natură a produce efecte.

Față de toate acestea, în opinia instanței, folosirea numelui unei alte persoane pentru deschiderea unui cont în rețeaua facebook sau pornhub nu are ca rezultat *date necorespunzătoare adevărului*, astfel încât o astfel de acțiune nu îndeplinește această cerință esențială pentru existența infracțiunii de fals informatic.

Evident, deschiderea și folosirea unui cont pe o astfel de rețea publică, utilizând numele altei persoane, poate să realizeze conținutul altor infracțiuni, în măsura în care sunt întrunite elementele constitutive ale acestora (spre exemplu, înșelăciune), însă, în opinia instanței, nu sunt realizate condițiile de tipicitate ale infracțiunii de fals informatic, prevăzute de art. 325 din Codul penal.

III. **Punctele de vedere exprimate de curțile de apel și instanțele din circumscripțiile acestora cu privire la chestiunea de drept a cărei dezlegare se solicită**

Au comunicat puncte de vedere asupra problemei de drept în discuție curțile de apel Brașov, București, Constanța, Craiova, Galați, Iași, Oradea, Pitești, Târgu Mureș și Timișoara, care, după caz, au făcut referire și la punctele de vedere ale unora dintre instanțele arondate.

S-au conturat următoarele opinii:

III.1. **Într-o opinie majoritară**, exprimată de Curtea de Apel Brașov, Curtea de Apel București (Tribunalul București, Tribunalul Ialomița, Tribunalul Teleorman, Judecătoria Alexandria, Judecătoria Bolintin-Vale, Judecătoria Cornetu, Judecătoria Giurgiu, Judecătoria Roșiori de Vede, Judecătoria Turnu Măgurele, Judecătoria Videle, Judecătoria Zimnicea), Curtea de Apel Constanța (Tribunalul Constanța), Curtea de Apel Craiova (Tribunalul Dolj), Curtea de Apel Galați (Judecătoria Brăila), Curtea de Apel Iași (Tribunalul Iași, Tribunalul Vaslui, Judecătoria Huși, Judecătoria Iași), Curtea de Apel Oradea (Judecătoria Carei, Judecătoria Negrești-Oaș) și Curtea de Apel Timișoara (Tribunalul Arad, Tribunalul Caraș-Severin, Tribunalul Timiș, Judecătoria Caransebeș), s-a susținut că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), nu realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal.

În susținerea acestei orientări, instanțele au achiesat la argumentele reținute de Curtea de Apel Brașov, astfel cum se regăsesc în încheierea de sesizare a Înaltei Curți de Casație și Justiție.

III.2. **În opinia minoritară**, exprimată de Curtea de Apel București — Secția a II-a penală (Tribunalul Giurgiu, Tribunalul Ilfov, Judecătoria Slobozia), Curtea de Apel Iași (Judecătoria Bârlad), Curtea de Apel Pitești, Curtea de Apel Târgu Mureș și Curtea de Apel Timișoara (Judecătoria Reșița, Judecătoria Timișoara), s-a apreciat că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea

de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului.

În susținerea acestei opinii s-a arătat că datele introduse răspund exigențelor art. 181 alin. (2) din Codul penal, constituie date informatice și sunt utilizate fără drept, întrucât noțiunea „fără drept” se referă la utilizarea datelor persoanei vătămate (nume, fotografii etc.), iar nu la dreptul de a utiliza sistemul informatic.

În situația deschiderii și utilizării unui cont pe o rețea de socializare deschisă publicului, fără drept, furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană, informațiile ce vizează acea persoană sunt folosite fără acordul acesteia din urmă, în sensul că sunt postate în spațiul public informații despre o persoană care nu și-a dat acordul și, astfel, cel ce le utilizează nu are acest drept.

Chiar dacă s-ar aprecia că sintagma „fără drept” nu poate fi avută în vedere în referire la persoana vătămată, faptul că rețeaua de socializare nu are mecanisme de verificare tehnică a corectitudinii datelor introduse de persoana care creează contul nu poate echivala cu acordul acelei rețele pentru crearea de conturi fictive, ci cu o încredere a rețelei respective că utilizatorii sunt de bună-credință și vor utiliza date reale la crearea conturilor.

Acțiunea are ca rezultat date necorespunzătoare adevărului, întrucât, deși datele sunt reale, nu este reală, în esență, voința de publicare a acestora.

În cadrul acestei opinii s-au formulat observații în sensul că nu ar fi întrunită condiția sub aspectul producerii de consecințe juridice, una dintre opinii fiind în sensul că încadrarea corectă ar fi fost în infracțiunea prevăzută de art. 226 alin. (2) din Codul penal.

O altă opinie, *minoritar exprimată*, a fost în sensul că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic prevăzută de art. 325 din Codul penal, cu referire la cerința ca acțiunea de introducere a unor date informatice să fie realizată fără drept, însă nu și sub aspectul condiției de a avea ca rezultat date necorespunzătoare adevărului.

În acest sens s-a avut în vedere faptul că datele introduse sunt corespunzătoare adevărului.

IV. Examenul jurisprudenței

Au fost atașate punctelor de vedere formulate de către instanțe hotărâri judecătorești pronunțate în această materie de către *Curtea de Apel Brașov* (Decizia penală nr. 639/2019; Decizia penală nr. 234/2020) și *Tribunalul Olt* (Sentința penală nr. 284/2015).

În considerentele Deciziei penale nr. 639/2019 pronunțate de Curtea de Apel Brașov — Secția penală s-a arătat că acțiunea reținută de procuror ca întrunind elementele constitutive ale infracțiunii prevăzute de art. 325 din Codul penal (constând în aceea că, în jurul datei de 27 noiembrie 2018, acționând din răzbunare și cu intenția de a produce consecințe juridice prin denigrarea persoanei vătămate în planul relațiilor sociale, inculpatul a creat un cont de Instagram fals cu denumirea (...), în care a introdus fără drept date informatice constând în informații și fotografii privind-o pe persoana vătămată B.N., rezultând astfel date necorespunzătoare adevărului, după care i-a invitat pe cei care urmăreau contul real al persoanei vătămate să urmărească contul fals creat de acesta) reprezintă în fapt o modalitate de săvârșire a infracțiunii de violare a vieții private, prevăzute de art. 226 alin. (2) din Codul penal.

În cuprinsul Deciziei penale nr. 234/2020 pronunțate de Curtea de Apel Brașov — Secția penală, prin care s-a menținut soluția de achitare dispusă de către instanța de fond cu privire la infracțiunea prevăzută de art. 325 din Codul penal,

s-a reținut că „*în condițiile în care inducerea în eroare, prin asumarea identității unei alte persoane, nu a îmbrăcat forma unei alte infracțiuni (spre exemplu, să aibă ca urmare producerea unei pagube), nu sunt îndeplinite condițiile pentru reținerea existenței infracțiunii de fals informatic sau a unei alte fapte cu caracter penal. În acest sens, în măsura în care ar fi afectată viața privată a unei persoane, astfel cum s-a susținut în cuprinsul motivelor de apel, s-ar putea reține existența infracțiunii prevăzute de art. 226 din Codul penal, în măsura în care transmiterea sunetelor sau imaginilor la care face referire acest text de lege se realizează prin folosirea unui cont facebook.*”

Prin Sentința penală nr. 284/2015 a Tribunalului Olt — Secția penală s-a reținut că faptele inculpatului de a introduce date informatice necorespunzătoare adevărului, creând un site fictiv din perspectiva apartenenței acestuia unei societăți de transport, pe care a postat un anunț de vânzare fictiv privind un autovehicul pe care în realitate nu îl deținea, în scopul obținerii pentru sine a unui folos patrimonial injust, pricinuind o pagubă de 4.000 euro cetățeanului spaniol P.L.G.G., întrunesc elementele constitutive ale infracțiunilor de fals informatic și de înșelăciune, prevăzute de art. 325 din Codul penal și art. 244 alin. (1) din Codul penal.

V. Punctul de vedere al Parchetului de pe lângă Înalta Curte de Casație și Justiție

Cu Adresa nr. 1.747/C/2390/III-5/2020 din data de 14 octombrie 2020, Parchetul de pe lângă Înalta Curte de Casație și Justiție — Secția judiciară — Serviciul judiciar penal a înaintat concluziile formulate asupra chestiunii de drept a cărei dezlegare s-a solicitat, comunicând, totodată, că nu există în lucru nicio sesizare având ca obiect promovarea unui recurs în interesul legii privind această chestiune de drept.

În esență, s-a susținut că problema de drept care se cere dezlegată urmărește a clarifica noțiunile „fără drept” și „date necorespunzătoare adevărului”, ca elemente de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal.

În ceea ce privește noțiunea „fără drept”, așa cum însăși instanța de sesizare a reținut, în absența unei explicații asupra a ceea ce legiuitorul a avut în vedere ca fiind fără drept, se aplică înțelesul noțiunii așa cum este reglementat în art. 35 alin. (2) din cap. I „Dispoziții generale”, titlul III „Prevenirea și combaterea criminalității informatice” din Legea nr. 161/2003.

Și în literatura de specialitate s-a reținut că noțiunea „fără drept” este definită, în cadrul Legii nr. 161/2003, în art. 35 alin. (2) lit. c), arătându-se că acționează fără drept acea persoană care nu are permisiunea din partea persoanei fizice sau juridice competente să o acorde.

A acționa fără drept înseamnă atât utilizarea fără drept a unui sistem informatic și a programului informatic aferent unei rețele de socializare, cât și introducerea fără drept în sistemul informatic a datelor informatice aparținând unei alte persoane.

S-a susținut că, în accepțiunea Legii nr. 161/2003, noțiunea de a acționa este o noțiune generală, care include toate modalitățile alternative de a introduce, modifica, șterge date informatice ori de a restricționa accesul la aceste date.

Noțiunea de a acționa cu sau fără drept nu poate fi limitată doar la dreptul de a utiliza un sistem informatic și programul informatic deoarece, pentru a fi întrunite cerințele de tipicitate ale infracțiunii de fals informatic, este necesar să rezulte date necorespunzătoare adevărului.

Pentru a acționa „cu drept”, persoana competentă trebuie să fie deținătoarea nu numai a sistemului informatic, dar și a datelor informatice.

Pe cale de consecință, noțiunea „fără drept” se raportează și la datele informatice, așa cum sunt definite prin dispozițiile art. 181 alin. (2) din Codul penal. Or, dacă aceste date informatice aparțin unei alte persoane decât utilizatorului de drept al sistemului informatic, este necesar ca acesta din urmă să aibă autorizarea sau permisiunea titularului datelor respective. În caz contrar, deținătorul sistemului informatic va introduce, modifica, șterge date informatice sau restricționează accesul la aceste date, fără drept.

În ceea ce privește noțiunea de date necorespunzătoare adevărului, s-a reținut în doctrină că aceasta este reglementată ca urmare imediată a acțiunilor de introducere, modificare, ștergere, fără drept, a datelor informatice ori de restricționare, fără drept, a accesului la aceste date. Astfel, urmarea imediată constă în obținerea de date informatice care nu au un corespondent în realitate și, prin aceasta, în crearea unei stări de pericol pentru încrederea care se acordă acestora și, în general, prelucrărilor automate de informații și pentru încrederea publicului în veridicitatea datelor informatice.

Datele rezultate sunt necorespunzătoare adevărului, adică date mincinoase, atunci când prezintă denaturat, altfel decât în realitate, fapta, informația la care se referă, respectiv o deformare a realității.

S-a apreciat în doctrină că inclusiv crearea unui profil fals în cadrul unei rețele de socializare poate atrage tipicitatea textului de incriminare. În măsura în care profilul fals implică utilizarea datelor de identificare ale unei persoane reale care nu și-a dat acordul în acest sens, se poate discuta de furt de identitate. Astfel, se reține infracțiunea de fals informatic în sarcina persoanei care, într-o rețea electronică socială (structură socială virtuală care oferă facilități de interacțiune membrilor săi înregistrați, permite schimbul de mesaje, date sau informații personale ori de interes general, de exemplu, Facebook etc.), creează un cont fictiv pe numele unei alte persoane, postând fotografia acesteia (reală sau modificată — de exemplu, într-o ipostază indecentă ori provocatoare), alături de informații personale (reale sau fabricate) care, prin natura lor, pot cauza prejudicii acesteia sau pot produce inclusiv consecințe juridice. În literatura de specialitate s-a considerat că acesta apare ca un caz tipic de „furt de identitate”.

Urmarea săvârșirii faptei constând în date necorespunzătoare adevărului reprezintă o abordare modernă, întrucât se bazează pe teoria intelectuală a conceptului de fals. Potrivit acestei teorii, există o infracțiune de fals atunci când se falsifică o manifestare de voință.

Din pct. 81 al Raportului explicativ al Convenției Consiliului Europei privind criminalitatea informatică rezultă faptul că legiuitorul european s-a raportat la aceeași teorie intelectuală a falsului. Astfel, importantă este falsificarea voinței titularului datelor informatice asupra cărora se acționează ori a persoanei care are vreun drept raportat la acestea — de exemplu, a persoanelor care au creat ori puteau să creeze (dar nu au făcut-o) în mod legitim respectivele date, a celor care au drept de modificare etc.

Potrivit pct. 83 din Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică, introducerea neautorizată a unor date corecte sau incorecte corespunde situației falsificării unui document.

Rezultă că atunci când sunt introduse pe o rețea de socializare date reale vizând o persoană (informații, fotografii, imagini video) într-un cont deschis pe numele acelei persoane, de către altcineva, fără acordul titularului datelor respective, urmarea o reprezintă date necorespunzătoare adevărului în privința titularului aceluși cont.

În această situație, nu este corespunzătoare adevărului împrejurarea că deținătorul legal al datelor informatice a deschis contul pe rețeaua de socializare și a introdus chiar el datele informatice. Lipsa acordului deținătorului legal al datelor informatice ca o altă persoană să introducă datele respective determină caracterul necorespunzător adevărului al acelor date.

În concluzie, s-a solicitat pronunțarea unei decizii prin care chestiunea de drept supusă dezlegării să primească următoarea rezolvare:

„Fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, acțiunea de introducere a unor date informatice fiind realizată fără drept, având ca rezultat date necorespunzătoare adevărului”.

VI. Punctul de vedere al Direcției legislație, studii, documentare și informatică juridică din cadrul Înaltei Curți de Casație și Justiție

Cu Adresa nr. 1.417 din data de 1 octombrie 2020, Direcția legislație, studii, documentare și informatică juridică din cadrul Înaltei Curți de Casație și Justiție a înaintat punctul de vedere asupra chestiunii de drept a cărei dezlegare s-a solicitat, apreciind că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, furnizând ca nume de utilizator numele unei alte persoane și introducând date cu caracter personal reale privind această persoană, întrunește elementele de tipicitate obiectivă ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, atât cu referire la cerința ca acțiunea de introducere a datelor informatice să fie realizată fără drept, cât și cu privire la cerința ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului.

În argumentarea acestei opinii s-a arătat că cerința ca acțiunea de introducere a datelor informatice să fie realizată fără drept are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003.

Făptuitorul care introduce într-o rețea de socializare deschisă publicului numele și datele cu caracter personal reale ale unei alte persoane, ca fiind datele privind propria identitate, introduce date informatice fără drept, în accepțiunea dispozițiilor art. 35 alin. (2) lit. a) din Legea nr. 161/2003, potrivit cărora acționează fără drept persoana care nu este autorizată, în temeiul legii sau al unui contract. Făptuitorul care introduce datele informatice privind identitatea reală a unei alte persoane și orice date cu caracter personal reale ale unei alte persoane, fără acordul acesteia, ca fiind datele informatice privind propria persoană, acționează fără drept, întrucât nu este autorizat în temeiul legii sau al unui contract să realizeze acțiunea de introducere a datelor informatice.

În primul rând, făptuitorul nu este autorizat în temeiul legii, întrucât nu există nicio dispoziție legală care să autorizeze o persoană să introducă date informatice privind o altă persoană (date informatice de identificare și alte date cu caracter personal reale), ca fiind date informatice privind propria persoană, într-o rețea de socializare deschisă publicului. Dimpotrivă, introducerea și utilizarea datelor informatice reale privind o altă persoană (numele și orice date cu caracter personal reale ale unei alte persoane) ca fiind date informatice privind propria persoană, într-o rețea de socializare deschisă publicului, se înscrie în fenomenul denumit „furt de identitate” și, în general, rețelele de socializare deschise publicului conțin o indicație privind raportarea conduitelor care se înscriu în acest fenomen.

În al doilea rând, făptuitorul nu este autorizat în temeiul unui contract, întrucât nu există acordul de voință al persoanei căreia îi aparțin datele informatice de identificare și alte date cu caracter personal reale introduse în rețeaua de socializare deschisă publicului.

În consecință, făptuitorul care introduce într-o rețea de socializare deschisă publicului numele și datele cu caracter personal reale ale unei alte persoane, ca fiind date privind propria identitate, nu este autorizat nici în temeiul legii și nici în temeiul unui contract, acționând fără drept, în sensul dispozițiilor art. 35 alin. (2) lit. a) din Legea nr. 161/2003.

În acest context, s-a precizat că „autorizarea” prevăzută în art. 35 alin. (2) din Legea nr. 161/2003 nu privește numai autorizarea generală de a introduce date informatice într-o rețea, ci și autorizarea de a introduce anumite categorii de date informatice într-o rețea. De exemplu, un funcționar bancar are autorizarea generală de a introduce date informatice în rețeaua băncii, dar nu are autorizarea de a introduce în rețeaua băncii datele unei persoane cu care banca nu are niciun raport contractual. În cazul rețelelor de socializare deschise publicului există, în principiu, o autorizare generală de a introduce date informatice în rețea, dar nu există nici autorizarea de a introduce datele unei alte persoane fără acordul acesteia și nici autorizarea de a introduce date informatice cu încălcarea unei interdicții (de exemplu, materiale cu caracter rasist sau xenofob).

Referitor la cerința ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului, s-a arătat că dispozițiile art. 325 din Codul penal (ca vechile dispoziții ale art. 48 din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției) transpun în dreptul intern prevederile art. 7 din Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, ratificată prin Legea nr. 64/2004.

Examinarea dispozițiilor art. 7 din Convenția Consiliului Europei privind criminalitatea informatică și ale art. 325 din Codul penal conduce la concluzia că expresia „date neautentice” a fost transpusă în dreptul intern prin expresia „date necorespunzătoare adevărului”.

În Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică, cu privire la art. 7, se precizează că neautenticitatea se referă, ca minim standard, la emitentul datelor, indiferent de exactitatea sau veridicitatea datelor.

Așadar, „datele neautentice” rezultate (în sensul art. 7 din Convenția Consiliului Europei privind criminalitatea informatică) și „datele necorespunzătoare adevărului” rezultate (în sensul art. 325 din Codul penal) privesc, în primul rând, emitentul datelor, astfel încât ori de câte ori nu există o identitate între persoana care introduce datele ca fiind date proprii și persoana căreia îi aparțin în mod real datele introduse există un fals informatic. „Datele neautentice” sau „datele necorespunzătoare adevărului” rezultate constau în inexistența identității de persoană între făptuitorul care introduce datele ca fiind date proprii și persoana căreia îi aparțin în mod real datele introduse.

Or, în cazul introducerii de către făptuitor, într-o rețea de socializare deschisă publicului, a numelui și a datelor cu caracter personal reale ale unei alte persoane ca fiind date privind propria identitate, rezultă inexistența unei identități de persoană între făptuitor și persoana căreia îi aparțin, în realitate, datele introduse și, pe cale de consecință, rezultă „date neautentice” în accepțiunea art. 7 din Convenția Consiliului Europei privind criminalitatea informatică sau „date necorespunzătoare adevărului” în accepțiunea art. 325 din Codul penal, fiind întrunită această cerință a infracțiunii de fals informatic.

Falsul informatic nu implică, în mod necesar, caracterul neautentic ori necorespunzător adevărului al datelor (numele

sau orice alte date cu caracter personal pot fi reale), ci include caracterul neautentic ori necorespunzător adevărului cu privire la emitentul datelor, astfel încât ori de câte ori făptuitorul, ca emitent al datelor, introduce date privind o altă persoană (date de identificare și alte date cu caracter personal reale), ca fiind date privind propria persoană, există un fals informatic.

VII. **Opinia specialiștilor consultați**

În conformitate cu dispozițiile art. 476 alin. (10) din Codul de procedură penală raportat la art. 473 alin. (5) din Codul de procedură penală, a fost solicitată opinia scrisă a specialiștilor din domeniul juridic cu privire la chestiunea de drept ce formează obiectul sesizării.

Facultatea de Drept din cadrul Universității București a opinat în sensul că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), nu realizează condiția de tipicitate a infracțiunii de fals informatic prevăzute de art. 325 din Codul penal, cu referire la realizarea fără drept a introducerii de date informatice, și nici condiția ca acțiunea să aibă ca rezultat date necorespunzătoare adevărului.

Referitor la elementul de tipicitate constând în realizarea introducerii de date informatice „fără drept” s-a arătat că sintagma menționată trebuie să fie interpretată prin intermediul dispozițiilor art. 35 alin. (2) din Legea nr. 161/2003, având în vedere faptul că infracțiunea de fals informatic a fost preluată în anul 2014 din respectivul act normativ în Codul penal.

A priori, s-a constatat că fapta nu este una în cazul căreia să se identifice o condiție legală de autorizare. Așadar, prima teză a lit. a) a art. 35 alin. (2) din Legea nr. 161/2003 este inaplicabilă. Având în vedere faptul că lit. b) a art. 35 alin. (2) din Legea nr. 161/2003 are drept premisă preexistența unei autorizări speciale, ale cărei limite sunt depășite, de asemenea, prin raportare la „autorizarea în temeiul legii”, s-a constatat inaplicabilitatea la problema pendinte.

În ceea ce privește lit. c) a art. 35 alin. (2) din Legea nr. 161/2003, s-a arătat că, în cazul unor rețele de socializare, nu se poate pune în discuție necesitatea unei permisiuni generale de folosire, administrare sau control al sistemului informatic. Dimpotrivă, proprietarii și administratorii rețelelor de socializare, prin natura acestui serviciu, operează cu premise de adresabilitate generală. Orice persoană își poate crea un cont fără a fi necesară o permisiune prealabilă din partea proprietarului sau administratorului rețelei de socializare (sau site-ului, în situații asimilabile), acesta fiind chiar scopul (de cele mai multe ori, comercial) acestor persoane fizice sau juridice. În concluzie, nici lit. c) a art. 35 alin. (2) din Legea nr. 161/2003 nu este aplicabilă în prezenta chestiune de drept.

În consecință, singura ipoteză care mai poate conduce la eventuala concluzie a unei acțiuni „fără drept” este cea prevăzută de teza a II-a a lit. a) a art. 35 alin. (2) din Legea nr. 161/2003, respectiv lipsa unei autorizări în temeiul unui contract.

S-a susținut însă că sintagma „fără drept” se cuvine a fi înțeleasă prin intermediul înțelegerii de ansamblu a scopului legiuitorului în momentul incriminării falsului informatic. Nu întâmplător legiuitorul a inclus falsul informatic în capitolul „falsuri în înscrisuri”. Astfel, din punctul de vedere al obiectului juridic generic și al *ratio legis* se impune ca interpretarea falsului informatic să fie consonantă cu interpretarea celorlalte infracțiuni din capitol.

Un aspect comun al tuturor celorlalte infracțiuni este acela că înscrisurile/înregistrările tehnice/declarațiile/actele ce servesc la identificare, legitimare ori la dovedirea stării civile au

aptitudinea, chiar prin natura lor, de a produce consecințe juridice.

Pe de altă parte, situația de fapt generică asupra căreia se apleacă prezenta chestiune de drept (respectiv utilizarea identității unei alte persoane în contextul unui cont creat pe o rețea de socializare) conduce spre o privire comparativă cu infracțiunea de fals privind identitatea (art. 327 din Codul penal). Se constată că legiuitorul a înțeles să incrimineze fapta unei persoane de a-și atribui identitatea unei alte persoane numai în contextul în care acțiunea se realizează în fața unei persoane dintre cele prevăzute la art. 175 din Codul penal sau unei unități în care aceasta își desfășoară activitatea, respectiv într-un context care prin natura sa este deja generator de consecințe juridice.

Nu se întrevide niciun motiv pentru care limitele și sfera de incriminare a falsului informatic să fie în mod exagerat lărgite prin comparație. La momentul incriminării faptei, legiuitorul a avut în vedere tranziția spre digitalizare, spre informatizare, urmărind să creeze o infracțiune care să opereze ca o opțiune paralelă față de celelalte incriminări din capitol, dar aplicabilă în mediul virtual.

Din aceste motive, și sintagma „fără drept” trebuie să fie înțeleasă în același sens, respectiv referindu-se la introducerea de date informatice care, prin natura lor, să aibă aptitudinea de a produce consecințe juridice.

Având în vedere scopul existenței rețelelor de socializare de tip Facebook, precum și faptul că în cazul acestora nici nu se solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont, faptul că datele informatice introduse în momentul creării unui cont și postării de conținut în respectivul cont nu sunt date care prin natura lor să aibă aptitudinea de a produce consecințe juridice, nesubsumându-se astfel obiectului juridic generic al capitolului și neintrând în *ratio legis* al incriminării, s-a apreciat că nu este îndeplinit nici elementul de tipicitate „fără drept”, astfel cum art. 35 alin. (2) din Legea nr. 161/2003 trebuie interpretat prin raportare la art. 325 din Codul penal.

În ceea ce privește elementul de tipicitate constând în rezultatul unor date necorespunzătoare adevărului, s-a arătat că sensul sintagmei „date necorespunzătoare adevărului” nu trebuie să fie doar acela de trucidare a unor date informatice, ci și de necorespondență între datele informatice și realitate.

Astfel, *lato sensu* (însă nu în sensul elementului de tipicitate al infracțiunii, astfel cum acesta trebuie să fie limitat), împrejurarea că o persoană creează un cont cu numele altei persoane și postează imagini ale acestei alte persoane generează o necorespondență între datele informatice și realitate. Deși ceilalți utilizatori ai rețelei de socializare vor crede că respectivul cont a fost manifestarea de voință a celui al cărui nume apare ca titular de cont, în realitate acesta aparține altei persoane. Rezultă în acest mod date necorespunzătoare adevărului.

S-a arătat însă că expresia „date necorespunzătoare adevărului”, în sensul infracțiunii de fals informatic, trebuie să fie interpretată limitat la obiectul juridic și la *ratio legis* al incriminării. Datele necorespunzătoare adevărului, *stricto sensu*, trebuie să se refere la date a căror necorespondență cu adevărul să fie prin natura lor apte să genereze consecințe juridice. Cu alte cuvinte, operând comparația cu celelalte infracțiuni de falsuri în înscrisuri, necorespondența datelor cu realitatea trebuie să fie similară cu situația necorespondenței unui înscris oficial sau a unui înscris sub semnătură privată (astfel cum sunt acestea caracterizate ca obiecte materiale ale infracțiunilor) cu realitatea.

Drept urmare, s-a apreciat că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către

deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), nu realizează condiția de tipicitate a infracțiunii de fals informatic cu referire la cerința ca acțiunea să aibă ca rezultat date necorespunzătoare adevărului.

Facultatea de Drept din cadrul Universității Lucian Blaga din Sibiu a arătat că, în conformitate cu cerința legii ca acțiunea de introducere a datelor să fie realizată „fără drept”, fapta reținută în sarcina inculpatului întrunește această condiție, întrucât incriminarea a fost preluată în Codul penal din Legea nr. 161/2003.

Raportat la dispozițiile art. 35 alin. (2) din Legea nr. 161/2003 și art. 35 alin. (1) din același act normativ, s-a apreciat că, în cauza dedusă judecătii, inculpatul a introdus date informatice într-un sistem informatic prin crearea unui cont fals pe o rețea de socializare deschisă publicului (într-un sistem informatic accesibil oricărei persoane), fără a avea acordul persoanei reale a cărei identitate a utilizat-o.

Referitor la cea de-a doua cerință a legii, ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului, s-a considerat că și aceasta este îndeplinită.

Așa cum rezultă din cuprinsul dispozițiilor art. 35 alin. (1) lit. d) din Legea nr. 161/2003, prin „date informatice” se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include și orice program informatic care poate determina realizarea unei funcții de către un sistem informatic. Pe cale de consecință, cerința art. 325 din Codul penal, care incriminează falsul informatic, se referă la „datele informatice”, chiar dacă în conținutul normei legiuitorul utilizează prima dată sintagma completă „date informatice” și ulterior, de încă două ori, doar cuvântul „date”.

Ca atare, în noțiunea de „date informatice” intră și conținutul de pe o rețea de socializare care se constituie într-o reprezentare a unor date, informații despre o anumită persoană. Doar persoana în cauză poate să dispună cum dorește de datele, informațiile și imaginile care o privesc și poate să decidă care dintre acele informații, date sau imagini să le facă publice. În speță, inculpatul a creat conturile de pe acele rețele, inducând în mod fals în percepția publicului aparența că persoana vătămată și-a creat singură acel profil, pe rețelele de socializare, dintre care una era destinată consumatorilor de pornografie; în acest fel, acțiunea sa a produs, în mod direct, date necorespunzătoare adevărului, din moment ce persoana vătămată nici nu a creat personal acele profile, nici nu a autorizat pe altcineva să le creeze ori să le completeze cu anumite informații sau date. Chiar dacă imaginile, datele sau informațiile introduse de inculpat în sistemul informatic provin din relația anterioară cu persoana vătămată și sunt autentice, ele au fost utilizate pentru crearea unor profile nereale, care să servească scopurilor urmărite de inculpat și care să contureze o anumită imagine despre persoana vătămată. Datele necorespunzătoare adevărului se reflectă în acest caz în caracterul nereal, fals al profilului creat, a cărui realizare nu reprezintă manifestarea de voință a titularului și al cărui conținut nu a fost autorizat de titular.

Facultatea de Drept din cadrul Universității de Vest din Timișoara a arătat că, în ceea ce privește infracțiunea de fals informatic, în oricare dintre modalitățile prevăzute în art. 325 din Codul penal, sunt de observat trei condiții.

O primă condiție constă în introducerea, modificarea sau ștergerea fără drept de date informatice sau restricționarea, fără drept, a accesului la astfel de date.

Definirea noțiunilor de furnizor de servicii, date informatice și utilizator se regăsește în cuprinsul Legii nr. 161/2003.

Art. 35 alin. (2) lit. a) din cuprinsul aceleiași legi definește sintagma „fără drept” folosită în norma de incriminare a falsului informatic. Potrivit acestui text de lege, acționează fără drept un utilizator „care nu este autorizat, în temeiul legii sau al unui contract”. Acțiunea de introducere, modificare sau ștergere de date informatice este fără drept, atunci când există obligația inserării unor date reale privind identitatea, obligație instituită printr-o autorizație sau contract. În cazul falsului informatic, noțiunea fără drept reprezintă un element de tipicitate, iar nu unul de antijuridicitate/cauză justificativă — exercitarea unui drept ori consimțământul persoanei vătămate.

În consecință, problema trebuie nuanțată raportat la politica de utilizare a fiecărei platforme.

În ipoteza în care rețeaua de socializare nu condiționează crearea unui cont de utilizarea numelui real și nici nu interzice utilizatorului să își atribuie datele de identitate ale altei persoane, prin prisma unor relații contractuale între utilizatorul rețelei și furnizorul rețelei, condiția de a acționa fără drept nu este îndeplinită.

În cazul rețelei de socializare care permite deschiderea unui cont folosind un alt nume sau un pseudonim, dar instituie obligația de a nu prelua identitatea altora sau furnizarea de informații inexacte, condiția este îndeplinită. Utilizatorul își asumă aceste obligații prin acceptarea condițiilor de utilizare a platformei, chiar dacă rețeaua de socializare nu solicită atașarea unui document de identitate. În aceste condiții, utilizatorul depășește o limită a autorizării contractuale, fiind irelevant că este solicitată sau nu și proba identității atribuite.

În fine, este evident fără drept atribuirea unei alte identități pe o platformă care permite doar folosirea datelor reale ale persoanei care le introduce și le folosește, indiferent că solicită sau nu dovada acestora.

Sintagma fără drept, folosită de legiuitor, se referă la acțiunea de introducere, ștergere, modificare sau restricționare, nu la acțiunea de deținere a datelor informatice sau la natura datelor. Nu acțiunea de deținere sau de folosire este incriminată, ci operațiunea tehnică de introducere, ștergere, modificare sau restricționare.

Cea de-a doua condiție, date necorespunzătoare adevărului, este consecința primei acțiuni, de introducere de date. Fapta de a introduce alte date decât cele personale are ca rezultat obținerea de date necorespunzătoare adevărului și, prin aceasta, crearea unei stări de pericol pentru încrederea care se acordă datelor informatice.

Denumirea infracțiunii este de natură a crea o ușoară confuzie, în sensul că sugerează că ar trebui să existe date false, însă textul de lege se abate de la această idee. Nu se referă la natura datelor sau la dreptul de a le folosi, ci la consecința pe care o produce introducerea unor date. Legiuitorul nu folosește sintagma date nereale, ci date necorespunzătoare adevărului. Date necorespunzătoare adevărului înseamnă date mincinoase care prezintă denaturat, altfel decât în realitate, fapta, informația la care se referă, respectiv o deformare a realității. În consecință, folosirea ca nume de utilizator a numelui unei alte persoane, lăsând să se înțeleagă că acea persoană este titularul contului, creează o percepție contrară realității.

Cu toate că datele de identificare ale persoanei vizate de deschiderea contului sunt reale, prin modul lor de folosire, al contextului în care sunt utilizate, acestea sunt date necorespunzătoare adevărului. Datele „atestă fapte ori situații de maniera prevăzută de persoana care dispune de ele, ajungându-se la o situație care corespunde fabricării unor documente false” [M. Dobrinou în V. Dobrinou (coord.), *Noul Cod penal comentat, Partea specială*, Ediția a II-a, Universul Juridic, 2014, p. 668].

Referitor la cea de-a treia condiție, constând în producerea unor consecințe juridice, s-a arătat că elementul esențial al

acestei infracțiuni este scopul, simpla acțiune de introducere de date, fie și nereale, nu produce automat consecințe juridice.

Acțiunea de introducere, modificare sau ștergere, fără drept, de date informatice, rezultând date necorespunzătoare adevărului, trebuie să vizeze producerea unor consecințe juridice în planul relațiilor sociale. Scopul trebuie să fie prestabilit. În măsura în care acțiunea nu are ca scop o atingere adusă vieții private a unei persoane, o lezare a dreptului la respectarea vieții private sau orice altă consecință juridică de natură a vătămă a persoanei, fapta nu este tipică.

Scopul producerii de consecințe juridice se verifică de la caz la caz, în funcție de circumstanțele concrete ale fiecărei cauze. Întrucât prezenta sesizare nu face referire la acest aspect, se poate prezuma că această cerință este îndeplinită.

Facultatea de Drept din cadrul Universității Babeș-Bolyai din Cluj-Napoca a opinat în sensul că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu necesită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzute de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului.

În sprijinul acestei opinii s-a arătat că infracțiunea de fals informatic, în modalitatea introducerii de date informatice, se aseamănă în mod esențial cu infracțiunea corespondentă de fals material în înscrisuri oficiale, în modalitatea contrafacerii de înscrisuri, prin faptul că în ambele situații se atribuie în mod nelegal o manifestare de voință unei persoane care nu a avut-o în fapt. Din acest punct de vedere, este lipsit de importanță faptul că o parte dintre datele informatice introduse (în speță, pozele sau identitatea) sunt reale, cât timp autorul creează falsa aparență că acestea sunt atribuibile unei alte persoane.

Având în vedere particularitățile normei în materie de fals informatic în modalitatea creării unui cont pe o rețea publică de socializare (ce presupune introducerea de date informatice) și a introducerii altor date informatice pe acel cont (în speță poze), acest raport de nonidentitate trebuie stabilit între identitatea aparentă a persoanei care a introdus aceste date (titularul aparent al contului) și identitatea efectivă a persoanei care a introdus respectivele date informatice. Mai exact, pentru a putea discuta despre introducerea unor date informatice neadevărate este necesar ca persoana care le-a introdus în mod efectiv să fie diferită de persoana care, în percepția publicului, este considerată creatorul/titularul acelor date informatice.

Este adevărat că o rețea publică de socializare nu cere de regulă garanții prealabile celui care introduce datele informatice referitor la realitatea identității pe care acesta o folosește (în sensul în care, spre exemplu, anterior creării contului, rețeaua nu solicită o copie a actului de identitate). Această împrejurare ar putea aparent să constituie și un eventual impediment pentru includerea unei astfel de conduite în infracțiunea de fals informatic, din perspectiva condiției de tipicitate fără drept din cadrul normei de incriminare.

S-a apreciat că lipsa unei astfel de cerințe privind „controlul prealabil” al identității nu implică automat faptul că rețeaua de socializare ar permite crearea unor conturi prin utilizarea identității unei alte persoane. Astfel, spre exemplu, rețeaua publică de socializare Facebook recomandă (aproape impune) folosirea identității reale de către utilizator și interzice folosirea serviciilor sale atunci când sunt încălcate „standardele comunității Facebook” sau atunci când există o conduită frauduloasă sau prin care se aduce atingere drepturilor altor persoane.

Referitor la „standardele comunității”, Facebook prevede într-o manieră explicită faptul că, pentru crearea contului, este interzisă folosirea unei alte identități decât a celei reale sau asumarea identității unei alte persoane prin folosirea/încărcarea unor imagini.

Chiar și dacă s-ar nega obligativitatea regulii privind utilizarea identității reale, considerând că aceasta ar fi o simplă recomandare a rețelei de socializare, care însă nu are nicio forță coercitivă atașată, simplul fapt că rețeaua publică de socializare nu ar impune existența unei astfel de identități (între creatorul efectiv al datelor informatice și titularul aparent al acestora) nu ar putea avea ca efect excluderea conduitei aici analizate de sub incidența textului de incriminare.

Un potențial efect care ar putea fi acceptat ar fi acela că o astfel de regulă, de facto permisivă, ar vulnerabiliza percepția terților raportat la aparența că titularul datelor informatice introduse corespunde la nivel de identitate cu persoana care figurează formal ca titular al contului. Totuși, un astfel de dubiu cu privire la identitate ar fi în mod cert anulat în condițiile în care cel care introduce datele informatice, respectiv numele și prenumele fals, nu se rezumă doar la această activitate ci, în „sușinerea” identității sale aparente, încarcă pe platforma de socializare poze reale ale titularului aparent al contului. Într-o atare ipoteză, este clar că în percepția terților dubiul cu privire la identitatea creatorului contului este mult mai scăzut, înspre inexistent, respectivul cont (și manifestarea de voință corespondentă) ajungând să fie atribuit în percepția terților persoanei care figurează formal ca titular al contului.

Așadar, deși folosirea unui „pseudonim” este un drept al oricărei persoane, nu este permis ca „exercitarea” acestui drept să aibă ca rezultat atribuirea identității unei alte persoane, care nu și-a dat acordul în acest sens. Din acest motiv, simpla creare a unui cont fictiv pe o rețea publică de socializare nu are *ab initio* semnificația unui fals informatic. În schimb, atribuirea aceluși cont unei alte persoane și postarea de fotografii ale persoanei a cărei identitate a fost uzurpată fraudulos presupune o falsificare a manifestării de voință a celui din urmă. Așadar, datele informatice introduse fraudulos, prin crearea aparenței că acel cont aparține unei alte persoane, intră în tipicitatea infracțiunii de fals informatic.

VIII. Dispoziții legale incidente

Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției

Art. 35.

„(2) În sensul prezentului titlu, acționează fără drept persoana care se află în una dintre următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depășește limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.”

Codul penal

Art. 181 — *Sistem informatic și date informatice*

„(1) Prin *sistem informatic* se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.

(2) Prin *date informatice* se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic.”

Art. 325 — *Falsul informatic*

„Fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste

date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoarea de la unu la 5 ani.”

IX. Raportul asupra chestiunii de drept supuse dezlegării

Opinia judecătorului-raportor este în sensul că fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește elementele de tipicitate obiectivă ale infracțiunii de fals informatic, prevăzută în art. 325 din Codul penal, atât cu referire la cerința ca acțiunea de introducere a datelor informatice să fie realizată fără drept, cât și cu referire la cerința ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului.

X. Înalta Curte de Casație și Justiție

Examinând sesizarea formulată de Curtea de Apel Brașov — Secția penală, prin care se solicită pronunțarea unei hotărâri prealabile, raportul întocmit de judecătorul-raportor și chestiunea de drept ce se solicită a fi dezlegată, reține următoarele:

X.1. Cu privire la admisibilitatea sesizării:

În conformitate cu dispozițiile art. 475 din Codul de procedură penală: „*Dacă, în cursul judecării, un complet de judecată al Înaltei Curți de Casație și Justiție, al curții de apel sau al tribunalului, investit cu soluționarea cauzei în ultimă instanță, constatând că există o chestiune de drept, de a cărei lămurire depinde soluționarea pe fond a cauzei respective și asupra căreia Înalta Curte de Casație și Justiție nu a statuat printr-o hotărâre prealabilă sau printr-un recurs în interesul legii și nici nu face obiectul unui recurs în interesul legii în curs de soluționare, va putea solicita Înaltei Curți de Casație și Justiție să pronunțe o hotărâre prin care să se dea rezolvare de principiu chestiunii de drept cu care a fost sesizată.*”

Din cuprinsul prevederilor legale care reglementează procedura de sesizare a Înaltei Curți de Casație și Justiție în vederea pronunțării unei hotărâri prealabile rezultă următoarele condiții de admisibilitate a sesizării, care trebuie îndeplinite cumulativ:

— chestiunea de drept să fie ridicată în cursul judecării, în fața unui complet de judecată al Înaltei Curți de Casație și Justiție, al curții de apel sau al tribunalului, investit cu soluționarea cauzei în ultimă instanță;

— chestiunea de drept să nu facă obiectul unui recurs în interesul legii în curs de soluționare, iar Înalta Curte de Casație și Justiție să nu fi statuat deja asupra problemei de drept printr-o hotărâre obligatorie pentru toate instanțele;

— chestiunea de drept pusă în discuție să fie una veritabilă, dificilă, susceptibilă să dea naștere unor interpretări diferite;

— chestiunea de drept să fie esențială, în sensul că de lămurirea ei depinde soluționarea pe fond a cauzei.

Înalta Curte constată că sunt îndeplinite condițiile prevăzute de art. 475 din Codul de procedură penală.

Astfel, Curtea de Apel Brașov — Secția penală este investită cu soluționarea dosarului în ultimă instanță, cauza se află în curs de judecată, iar problema de drept a cărei dezlegare se solicită nu a mai fost supusă examenului Înaltei Curți de Casație și Justiție, nici pe calea unei întrebări prealabile, nici printr-un recurs în interesul legii. Totodată, astfel cum rezultă din relațiile comunicate de Parchetul de pe lângă Înalta Curte de Casație și Justiție — Secția judiciară — Serviciul judiciar penal, nu există în lucru nicio sesizare având ca obiect promovarea unui recurs în interesul legii privind această chestiune de drept.

Întrebarea ce face obiectul sesizării reprezintă o veritabilă problemă de drept, care, prin gradul său de dificultate, necesită o dezlegare cu valoare de principiu din partea instanței supreme. O dovadă în acest sens o reprezintă divergențele de

opinii cu privire la interpretarea acesteia, rezultate în urma consultării instanțelor judecătorești și a specialiștilor din cadrul facultăților de drept.

Rezolvarea dată chestiunii de drept expuse în încheierea de sesizare este susceptibilă a avea consecințe juridice directe asupra modului de soluționare a cauzei, în condițiile în care aceasta vizează două dintre elementele de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, care constituie obiectul acuzației penale.

X.2. Cu privire la fondul sesizării:

Analiza din prezenta cauză este circumstanțiată situației în care făptuitorul introduce, prin crearea unui cont într-o rețea de socializare deschisă publicului, numele și datele personale reale ale altei persoane (date care permit identificarea — informații, fotografii, imagini video) fără acordul acesteia. Problema de drept vizează întrunirea sau nu a două dintre cerințele esențiale atașate elementului material al laturii obiective a infracțiunii de fals informatic, acelea ca fapta să fie săvârșită *fără drept* și să aibă ca rezultat *date necorespunzătoare adevărului*.

Prealabil verificării îndeplinirii acestor condiții de tipicitate obiectivă, se impun anumite considerații privind instrumentele juridice internaționale care au condus la incriminarea falsului informatic, acestea prezentând relevanță din perspectiva chestiunilor de drept asupra cărora instanța supremă este chemată să se pronunțe.

Incriminarea falsului informatic constituie materializarea demersului de transpunere în dreptul intern a prevederilor art. 7 din Convenția Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, ratificată prin Legea nr. 64/2004.

Potrivit dispozițiilor art. 7 din Convenția Consiliului Europei privind criminalitatea informatică, care se referă la „falsificarea informatică”, *fiecare parte va adopta măsurile legislative și alte măsuri care se dovedesc necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, introducerea, alterarea, ștergerea sau suprimarea intenționată și fără drept a datelor informatice, din care să rezulte date neautentice, cu intenția ca acestea să fie luate în considerare sau utilizate în scopuri legale ca și cum ar fi autentice, chiar dacă sunt sau nu sunt în mod direct lizibile și inteligibile. O parte va putea condiționa răspunderea penală de existența unei intenții frauduloase sau a unei alte intenții delictuale.*

În Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică, cu referire la art. 7, se rețin următoarele:

— **scopul acestui articol este de a crea o infracțiune paralelă cu falsificarea de documente tangibile**, pentru completarea lacunelor din dreptul penal legate de falsurile tradiționale, care necesită lizibilitatea vizuală a declarațiilor sau declarațiilor înscrise într-un document și care nu se aplică datelor stocate electronic. Falsificarea computerizată presupune crearea sau modificarea neautorizată a datelor stocate, astfel încât acestea să dobândească o valoare probatorie. Interesul juridic protejat este securitatea și fiabilitatea datelor electronice care pot avea consecințe pentru relațiile juridice (paragraful 81);

— conceptele naționale de falsificare variază foarte mult. Un concept se bazează pe autenticitatea cu privire la autorul documentului, iar altele se bazează pe veridicitatea declarației conținute în document. Cu toate acestea, s-a convenit că **neautenticitatea se referă cel puțin la emitentul datelor, indiferent de corectitudinea sau veridicitatea conținutului datelor**. Părțile pot merge mai departe și include sub termenul „autentic” autenticitatea datelor (paragraful 82);

— dispoziția acoperă datele care echivalează cu un document public sau privat, care are efecte juridice. **Introducerea neautorizată de date corecte sau incorecte despre o situație care corespunde realizării unui document**

fals. Modificări ulterioare (modificări, variații, modificări parțiale), ștergeri (ștergerea datelor dintr-un mediu de date) și suprimarea (reținerea, ascunderea datelor) **corespund în general falsificării unui document autentic** (paragraful 83);

— termenul „în scopuri legale” se referă și la tranzacțiile juridice și la documentele care sunt relevante din punct de vedere juridic (paragraful 84);

— teza finală a dispoziției permite părților să solicite în plus o intenție de fraudare sau o intenție necinstită similară, înainte de atașarea răspunderii penale (paragraful 85).

Dispozițiile art. 7 din Convenția Consiliului Europei privind criminalitatea informatică au fost transpuse în dreptul intern prin art. 48 din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției. Ulterior, textul a fost preluat în art. 325 din noul Cod penal, tipicitatea faptei rămânând neschimbată, singurele modificări vizând sancțiunea ale cărei limite au fost reduse.

Astfel, potrivit art. 325 din Codul penal, *„fapta de a introduce, modifica sau șterge, fără drept, date informatice ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecințe juridice, constituie infracțiune și se pedepsește cu închisoarea de la unu la 5 ani”*.

Având în vedere că prin incriminare s-a urmărit crearea unei infracțiuni paralele cu infracțiunile tradiționale de fals în înscrisuri, legiuitorul a inclus-o în capitolul consacrat „falsurilor în înscrisuri”.

Plecând tot de la apartenența la această categorie de infracțiuni, în ceea ce privește elementul material al laturii obiective, în doctrină s-a susținut că modalitatea *introducerii de date informatice* corespunde, în principiu, *contrafacerii unui document*, iar *modificarea, ștergerea, restricționarea accesului la datele informatice* corespund conceptului de *alterare* a unui document digital¹. La o concluzie similară se ajunge și în Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică (paragraful 83).

Examinând comparativ actuala reglementare națională și dispozițiile art. 7 din Convenția Consiliului Europei privind criminalitatea informatică, sub aspectul elementelor de tipicitate care interesează prezenta cauză, respectiv cerințele atașate elementului material al laturii obiective, acelea ca fapta să fie săvârșită *fără drept* și să aibă ca rezultat *date necorespunzătoare adevărului*, se constată că nu există diferențe. Sintagma „*date neautentice*” a fost transpusă în dreptul intern ca „*date necorespunzătoare adevărului*”, însă între cele două noțiuni nu există deosebiri, terminologia folosită de legiuitor fiind corespunzătoare celei utilizate în cazul infracțiunilor de fals în înscrisuri (art. 321, art. 322 și art. 326 din Codul penal).

A. Pornind de la aceste considerații, **în ceea ce privește cerința ca acțiunea de introducere a datelor informatice să fie realizată fără drept**, se rețin următoarele:

Potrivit art. 181 alin. (2) din Codul penal, prin *date informatice* se înțelege orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un *sistem informatic* [noțiune definită de alin. (1) al aceluiași articol].

Spre deosebire de Legea nr. 161/2003, care, în art. 35 alin. (2), reglementa înțelesul sintagmei „*fără drept*”, Codul penal, deși a preluat toate infracțiunile din titlul III — *Prevenirea și combaterea criminalității informatice* al cărții I — *Reglementări generale pentru prevenirea și combaterea corupției* din Legea nr. 161/2003, precum și o parte din definițiile date unor noțiuni („sistem informatic”, „date informatice”), nu cuprinde o dispoziție similară.

¹ Sergiu Bogdan, Doris Alina Șerban, George Zlati, *Noul Cod penal, Partea specială, Analize, explicații, comentarii, Perspectiva clujeană*, Editura Universul Juridic, București, 2014, pag. 559; Cristina Rotaru, Andra Roxana Trandafir, Valerian Cioclei, *Drept penal, Partea specială II, Curs tematic*, ediția 2, Editura C. H. Beck, 2018, pag. 402—403; George Zlati, *Tratat de criminalitate informatică*, vol. 1, Editura Solomon, 2020, pag. 513 și urm.

Având însă în vedere împrejurarea că prevederile art. 35 alin. (2) din Legea nr. 161/2003 nu au fost abrogate, ele continuă să aibă relevanță juridică din perspectiva incriminărilor preluate în noul Cod penal. Aceasta este poziția unitară a doctrinei, precum și a practicii judiciare și aceeași interpretare o regăsim și în jurisprudența Curții Constituționale. Astfel, efectuând controlul de constituționalitate cu privire la dispozițiile art. 360 din Codul penal referitoare la infracțiunea de acces ilegal la un sistem informatic, Curtea Constituțională precizează că infracțiunea a fost preluată din Legea nr. 161/2003 și explică cerința ca făptuitorul să acționeze fără drept prin referire la art. 35 alin. (2) din același act normativ, reținând că, „*chiar dacă Codul penal nu a preluat toate definițiile din Legea nr. 161/2003, aceasta rămâne în continuare un reper pentru înțelegerea elementelor de conținut ale infracțiunii criticate*” (Decizia nr. 183 din 29 martie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 486 din 13 iunie 2018).

Rezultă, așadar, că cerința ca acțiunea de contrafacere sau alterare a datelor informatice să fie realizată fără drept are semnificația atribuită prin dispozițiile art. 35 alin. (2) din Legea nr. 161/2003, respectiv: „(...) *acționează fără drept persoana care se află în una dintre următoarele situații:*

a) *nu este autorizată, în temeiul legii sau al unui contract;*

b) *depășește limitele autorizării;*

c) *nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.*”

În mod evident, dispozițiile art. 35 alin. (2) din Legea nr. 161/2003, comune unor incriminări distincte, trebuie analizate prin prisma elementului material al laturii obiective a fiecărei infracțiuni care are atașată această cerință esențială și pentru care textul este aplicabil.

În cazul falsului informatic, verificarea existenței sau nu a dreptului de a introduce, modifica sau șterge date informatice se impune a fi făcută prin raportare la persoana care are dreptul de dispoziție asupra acestor date, respectiv la existența sau nu a manifestării de voință a acesteia.

Analiza nu poate fi realizată din perspectiva existenței dreptului de a utiliza sistemul informatic (sau a condițiilor în care acesta poate fi utilizat). În cazul infracțiunii prevăzute de art. 325 din Codul penal, elementul material al laturii obiective nu se referă la o intervenție asupra unui sistem informatic, ci asupra unor date informatice. Sistemul informatic reprezintă doar mijlocul prin intermediul căruia se realizează falsul informatic, iar în măsura în care nu există o autorizare din partea titularului acestuia (în cauză, a titularului rețelei de socializare) eventual se pot ridica probleme din perspectiva unei alte incriminări, cea a accesului ilegal la un sistem informatic, prevăzută de art. 360 din Codul penal.

În ipoteza supusă analizei, făptuitorul care creează un cont/profil într-o rețea de socializare deschisă publicului, introducând numele și datele cu caracter personal reale ale altei persoane și care permit identificarea acesteia (informații, fotografii, imagini video etc.), ca fiind date referitoare la propria persoană, acționează prin încălcarea manifestării de voință a persoanei a cărei identitate și-a uzurpat-o. Informațiile introduse cu ocazia creării contului și cele conținute în diferite postări se circumscriu definiției prevăzute de art. 181 alin. (2) din Codul penal, fiind reprezentări care pot fi prelucrate prin sistemul informatic. Aceste date informatice sunt introduse *fără drept*, în accepțiunea dispozițiilor art. 35 alin. (2) lit. a) din Legea nr. 161/2003, potrivit cărora *acționează fără drept persoana care nu este autorizată, în temeiul legii sau al unui contract*.

Făptuitorul nu este autorizat în temeiul legii, pentru că nu există nicio dispoziție legală care să permită unei persoane să

introducă într-o rețea de socializare deschisă publicului date informatice privind o altă persoană (date de identificare și alte date cu caracter personal reale), ca fiind date privind propria persoană. Dimpotrivă, legea protejează dreptul la propria imagine (art. 73 din Codul civil), iar utilizarea, cu rea-credință, a numelui, imaginii sau vocii unei persoane constituie, potrivit art. 74 lit. h) din Codul civil, o atingere adusă vieții private.

De asemenea, făptuitorul nu este autorizat în temeiul unui contract, întrucât nu a fost mandatat în acest sens de persoana căreia îi aparțin datele informatice asupra cărora s-a acționat, nu există acordul de voință al acesteia.

În consecință, făptuitorul care, prin contrafacerea manifestării de voință a unei persoane, introduce într-o rețea de socializare deschisă publicului numele și datele cu caracter personal reale ale acesteia (și care permit identificarea sa), ca fiind date privind propria identitate, acționează *fără drept*, în sensul dispozițiilor art. 35 alin. (2) lit. a) din Legea nr. 161/2003. În fapt, situația reprezintă o ipoteză a „furtului de identitate”, care, similar clonării paginilor web (phishingul), intră sub incidența art. 7 din Convenția Consiliului Europei privind criminalitatea informatică [Nota de îndrumare nr. 4 a Comitetului Convenției privind criminalitatea informatică (T-CY) referitoare la *Furtul de identitate și phishingul în legătură cu fraudă*, adoptată la a noua sesiune plenară a T-CY, iunie 2013].

B. În ceea ce privește cerința ca acțiunea de introducere a datelor informatice să aibă ca rezultat date necorespunzătoare adevărului, problema de drept în discuție este dacă aceasta poate fi considerată îndeplinită în situația în care datele informatice introduse de făptuitorul care și-a uzurpat fraudulos identitatea unei alte persoane sunt reale, în sensul că acestora nu li s-au adus niciun fel de modificări.

Referitor la falsul în înscrisuri, în doctrină² s-a arătat că falsificarea materială include în sfera sa doar acele acțiuni care provoacă un raport de nonidentitate: în cazul *contrafacerii* nu va exista identitate între autorul aparent al înscrisului și cel de facto, în cazul *alterării* nu va exista identitate între conținutul inițial al manifestării de voință, cuprinsă în înscris, și cel rezultat în urma alterării. În abordarea clasică, falsul material a primit strict o dimensiune materială, considerându-se că există fals doar atunci când s-a modificat realitatea materială a unui înscris (teoria materială a falsului material). Falsul nu decurge însă, în mod automat, din diferențele în „materialitatea înscrisului”, ci el presupune constatarea unei inegalități între manifestările de voință (teoria intelectuală a falsului material). Astfel, în cazul alterării, trebuie analizat dacă există inegalitate între manifestarea de voință a emitentului la momentul întocmirii înscrisului și manifestarea de voință consemnată în scris după alterarea sa (de exemplu, nu va exista fals material în situația în care făptuitorul alterează înscrisul pentru a corecta o eroare materială cuprinsă în acesta, astfel încât el să corespundă cu manifestarea de voință reală a emitentului, cuprinsă inițial defectuos în înscris). În cazul contrafacerii, trebuie studiat dacă manifestarea de voință conținută în înscrisul contrafăcut are sau nu un corespondent în realitatea materială.

În ceea ce privește falsul informatic, prin includerea condiției ca acțiunea de contrafacere sau alterare a datelor informatice să fie făcută „fără drept”, legiuitorul intern, similar celui european (care a stabilit, ca minim standard, că neautenticitatea se referă cel puțin la emitentul datelor, indiferent de corectitudinea sau veridicitatea conținutului datelor³), s-a raportat la teoria intelectuală a falsului material.

Crearea unui cont fără drept, uzurpând identitatea unei persoane, prin introducerea de date reale și care permit identificarea respectivei persoane, presupune o falsificare a manifestării de voință a acesteia și creează o percepție contrară realității în privința titularului respectivului cont.

² Sergiu Bogdan, Doris Alina Șerban, George Zlati, *Noul Cod penal, Partea specială, Analize, explicații, comentarii, Perspectiva clujeană*, Editura Universul Juridic, București, 2014, pag. 539—540.

³ Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică, paragraful 82.

Așadar, *datele necorespunzătoare adevărului* rezultate privesc emitentul acestora și constau în lipsa concordanței între făptuitorul care introduce date ca fiind datele persoanei și persoana căreia acestea îi aparțin în realitate. Între datele informatice astfel contrafăcute (în modalitatea introducerii fără drept) și realitatea obiectivă nu există corespondență, manifestarea de voință reflectată de aceste date aparținând unei alte persoane (făptuitorului) decât celui care aparent este titular al contului (voința de publicare a datelor nu este reală).

În acest fel, introducerea unor date reale are ca rezultat date necorespunzătoare adevărului.

Concluzionând, condiția de tipicitate obiectivă analizată include și caracterul neautentic ori necorespunzător adevărului cu privire la emitentul datelor, astfel că ea este îndeplinită ori de câte ori datele obținute nu sunt în concordanță cu manifestarea de voință a persoanei căreia îi sunt atribuite.

Ca atare, prin introducerea într-o rețea de socializare deschisă publicului a numelui și a altor date personale reale ale unei alte persoane și care permit identificarea acesteia, ca și cum ar fi date privind propria identitate, rezultă *date necorespunzătoare adevărului* în accepțiunea art. 325 din Codul penal, fiind întrunită această cerință atașată elementului material al laturii obiective a infracțiunii de fals informatic.

Bineînțeles că pentru reținerea infracțiunii, pe lângă cele două cerințe esențiale ce fac obiectul analizei în prezenta sesizare, este necesar ca scopul activităților desfășurate *fără drept* și care au ca rezultat *date necorespunzătoare adevărului* să fie acela de a utiliza datele informatice în vederea producerii

de consecințe juridice, acesta urmând a fi verificat în funcție de circumstanțele concrete ale fiecărei cauze.

În considerarea celor expuse, Înalta Curte de Casație și Justiție — Completul pentru dezlegarea unor chestiuni de drept în materie penală va admite sesizarea formulată de Curtea de Apel Brașov — Secția penală în Dosarul nr. 9.010/197/2019, prin care se solicită pronunțarea unei hotărâri prealabile pentru dezlegarea chestiunii de drept: „Dacă fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.), realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului” și va stabili că:

Fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește două dintre cerințele esențiale ale infracțiunii de fals informatic prevăzute în art. 325 din Codul penal, respectiv cea ca acțiunea de introducere a datelor informatice să fie realizată **fără drept** și cea ca acțiunea de introducere a datelor informatice să aibă ca rezultat **date necorespunzătoare adevărului**.

ÎNALTA CURTE DE CASAȚIE ȘI JUSTIȚIE

În numele legii

DECIDE:

Admite sesizarea formulată de Curtea de Apel Brașov — Secția penală în Dosarul nr. 9.010/197/2019, prin care se solicită pronunțarea unei hotărâri prealabile pentru dezlegarea chestiunii de drept: „Dacă fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.) realizează condițiile de tipicitate ale infracțiunii de fals informatic, prevăzută de art. 325 din Codul penal, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului” și stabilește că:

Fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului, folosind ca nume de utilizator numele unei alte persoane și introducând date personale reale care permit identificarea acesteia, întrunește două dintre cerințele esențiale ale infracțiunii de fals informatic prevăzute în art. 325 din Codul penal, respectiv cea ca acțiunea de introducere a datelor informatice să fie realizată **fără drept** și cea ca acțiunea de introducere a datelor informatice să aibă ca rezultat **date necorespunzătoare adevărului**.

Obligatorie de la data publicării în Monitorul Oficial al României, Partea I, potrivit art. 477 alin. (3) din Codul de procedură penală. Pronunțată în ședință publică astăzi, 25 ianuarie 2021.

PREȘEDINTELE SECȚIEI PENALE
A ÎNALTEI CURȚI DE CASAȚIE ȘI JUSTIȚIE
judecător **DANIEL GRĂDINARU**

Magistrat-asistent,
Mihaela Ivănuș

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR



„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; C.I.F. RO427282,
IBAN: RO55RNCB0082006711100001 Banca Comercială Română — S.A. — Sucursala „Unirea” București
și IBAN: RO12TREZ7005069XXX000531 Direcția de Trezorerie și Contabilitate Publică a Municipiului București
(alocat numai persoanelor juridice bugetare)

Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, internet: www.monitoruloficial.ro

Adresa pentru publicitate: Centrul pentru relații cu publicul, București, șos. Panduri nr. 1,
bloc P33, parter, sectorul 5, tel. 021.401.00.73, fax 021.401.00.72

Tiparul: „Monitorul Oficial” R.A.



5 948493 321118