STUDIA UNIVERSITATIS MOLDAVIAE, 2020, nr.3(133)
Seria "Ştiinţe sociale" ISSN 1814-3199, ISSN online 2345-1017, p.139-151

CZU: 347.965.33(478) **DOI: 10.5281/zenodo.3886771**

PROTECȚIA JURIDICO-PENALĂ A SECRETULUI PROFESIONAL PRIN PRISMA INCRIMINĂRILOR PREVĂZUTE LA art.178, 259, 260[1], 260[2] CP RM

Costică MOȚOC, Lilia GÎRLA

Universitatea de Stat din Moldova

Scopul acestui articol rezidă în efectuarea unei analize juridice cuprinzătoare a semnelor obiective ale infracțiunilor prevăzute la articolele 178, 259, 260[1], 260[2] CP RM cu scopul de a cerceta plenitudinea și relevanța protecției juridico-penale a secretului profesional în legea penală a Republicii Moldova. În cadrul cercetării științifice s-a studiat literatura de specialitate, s-a analizat legislația extrapenală din Republica Moldova, s-au examinat actele internaționale în materia asigurării și protecției datelor personale confidențiale; s-au analizat semnele obiective ale faptelor infracționale prevăzute la articolele 178, 259, 260[1], 260[2] CP RM; s-a examinat practica judiciară; s-a cercetat plenitudinea și relevanța protecției juridico-penale a secretului profesional în legea penală a Republicii Moldova; s-a argumentat necesitatea revizuirii normelor care urmează a fi revizuite; s-au propus modificări *de lege ferenda* în scopul îmbunătățirii viitoare a legii penale.

Cuvinte-cheie: *secret primar, secret derivat, secret profesional, secretul corespondenței, corespondență electronică, acces la informații protejate, secretul vieții private.*

PENAL LEGAL PROTECTION OF THE PROFESSIONAL SECRET IN THE LIGHT OF THE ARTICLES 178, 259, 260[1], 260[2] OF THE CRIMINAL CODE OF THE REPUBLICA MOLDOVA

The basic purpose of this article consists in the detailed penal analysis of objective signs of the criminal offences provided in the articles 178, 259, 2601, 2602 Criminal code of the Republic of Moldova. The main task is considered to be the investigation of the relevant penal protection of professional secret in the Criminal Law of the Republic of Moldova. There have been researched the following sources: special scientific literature; national regulations as well as international treaties in the matter of confidential data protection. A special place is taken by the judicial practice. More than it, in the realm of this article the necessity for the further updating has been discussed, as a result, several amendments were proposed for the future improvement of the Criminal Law.

Keywords: *primary secret, secondary secret, professional secret, secret of communications, electronic communication, access to protected data, secret of privacy.*

Introducere

În cadrul acestui mesaj științific, ne-am propus următoarele obiective de cercetare: studierea literaturii de specialitate, analiza legislației extrapenale din Republica Moldova, examinarea actelor internaționale în materia asigurării și protecției datelor personale confidențiale; analiza semnelor obiective ale faptelor infracționale prevăzute la articolele 178, 259, 260[1], 260[2] CP RM; examinarea practicii judiciare; cercetarea plenitudinii și relevanței protecției juridico-penale a secretului profesional în legea penală a Republicii Moldova; identificarea normelor care urmează a fi revizuite; propunerea modificărilor *de lege ferenda* în scopul îmbunătățirii legii penale.

Astfel, dispoziția de la ***alin.(1) art.178 CP RM*** (Violarea dreptului la secretul corespondenţei) incriminează *violarea dreptului la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei*. Norma prevăzută la alin.(1) art.178 CP RM este o normă de blanchetă şi face referire la alin.(1) art.30 din Constituției Republicii Moldova, care prevede că statul asigură secretul convorbirilor telefonice.

Articolul 30 (Secretul corespondenței) din Constituția Republicii Moldova stipulează următoarele: ***alin.(1)*** – *Statul asigură secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare;* ***alin.(2)*** *– De la prevederile alineatului (1) se poate deroga prin lege în cazurile când această derogare este necesară în interesele securității naționale, bunăstării economice a țării, ordinii publice și în scopul prevenirii infracțiunilor.* De specificat că prevederile de la alin.(1) art.30 din Constituție conțin termeni și elemente importante pentru elucidarea conținutului sintagmei *„secretul corespondenței"*. Sintagma *„statul asigură"* semnalează existența unei obligații duble. Legea

ocrotește, deci, deopotrivă, orice corespondență, fie că include ceva tainic, fie că exprimă lucruri absolut lipsite de vreo doză de confidențialitate.

În sensul alin.(1) art.5 al Legii Republicii Moldova *privind comunicaţiile electronice,* nr.241 din 15.11.2007 [1], *confidenţialitatea convorbirilor telefonice sau a altor servicii de comunicaţii electronice, efectuate/furnizate prin reţelele de comunicaţii electronice, este asigurată de Constituţia Republicii Moldova, de această lege şi de alte legi*.

Potrivit alin.(2) art.5 al aceleiași legi, persoanele care activează în domeniul comunicaţiilor electronice au obligaţia să asigure confidenţialitatea specificată la alin.(1), interzicându-li-se divulgarea conţinutului convorbirilor telefonice şi al altor comunicări efectuate prin reţele de comunicaţii electronice, precum şi divulgarea informaţiilor privind serviciile furnizate altor persoane decât expeditorul sau destinatarul.

Rezultate și discuții

Inviolabilitatea secretului corespondenței al fiecărei persoane urmează a fi recunoscută în calitate de ***obiect juridic special*** al infracțiunilor prevăzute la art.178 CP RM. În acest context este relevant să menționăm că majoritatea autorilor ruși consideră că ***obiectul juridic special*** îl constituie relațiile sociale care asigură *dreptul persoanelor la secretul corespondenței, al convorbirilor și al altor comuncații* [2, p.46-47]. Însă, teoria obiectului infracțiunii, privit exclusiv ca relație socială, nu este oportună în mai multe situații; se acceptă teoria unei valori absolute, spre exemplu – personalitatea ca un ansamblu de relații sociale și personalitatea ca o valoare absolută. În acest mod, este trasată reîntoarcerea la abordarea obiectului protecției juridice nu doar în calitate de relație socială, dar și de valoare reală, interes real supus protecției juridico-penale [*Ibidem*].

Dreptul la inviolabilitatea secretului corespondenței personale constituie parte componentă a *dreptului la inviolabilitatea vieții private a persoanei* și, prin urmare, devine varietatea specială a obiectului de protecție juridico-penală, cum ar fi dreptul la secretul vieții personale și familiale. Cu toate acestea, *dreptul la secretul corespondenței personale* este parte integrantă a *dreptului la inviolabilitatea vieții private (personale sau familiale)* al unei persoane. Putem susține că dreptul la confidențialitatea corespondenței personale este un tip mai restrâns în comparație cu dreptul la intimitate privată [3, p.3]. Prin urmare, dacă culegerea datelor care constituie secret personal și familial al persoanei are loc prin încălcarea inviolabilității secretului de corespondență personală, atunci cele comise, reieșind din regula concurenței dintre norma generală și cea specială, se vor încadra în baza art.178 CP RM.

Autorul M.Dobrinoiu consemnează: *„Secretul corespondenței este un drept fundamental aflat în strânsă corelație cu dreptul la viața intimă și privată a persoanei. Viața privată și intimitatea unei persoane nu pot fi respectate fără o protecție a corespondenței private a acesteia"* [4]. Într-o opinie solidară întâlnită la autorul L.A. Țaturean, *secretul corespondenței* (cel al convorbirilor telefonice, al trimiterilor poștale, al telegramelor sau al altor comunicări) poate fi catalogat ca un *secret personal* [5, p.10-12]. Cu toate acestea, în timpul corespondenței pot avea loc convorbiri telefonice, poștale sau telegrafice, care pot să se refere nu doar la viața privată a unui individ, ci și la informații care constituie, de exemplu, secret comercial, fiscal, bancar, deci să fie de altă natură – *non-personală*. Astfel, autorul M.A.Erșov recomandă ca secretului corespondenței să i se atribuie un statut distinct de secret [6, p.103-104].

Corespondența în forma sa materială și imaterială constituie ***obiectul material/imaterial al infracțiunii în sensul art.178 CP RM***, însă nu toată. Dacă vom analiza noțiunea de corespondență în sensul ei generic și noțiunea de corespondență pentru toate categoriile de entități înscrise în dispoziția normei de la art.178 CP RM, vom concluziona că ele nu coincid. Asfel, în conformitate cu prevederile art.178 CP RM, prin corespondență se subînțeleg: scrisorile, telegramele, coletele și alte trimiteri poștale, convorbirile telefonice și înștiințările telegrafice, pe când alte forme de corespondență, cum ar fi corespondența electronică, nu se acoperă cu protecția juridico-penală în sensul art.178 CP RM.

În mod tradițional, în calitate de *corespondență* se înțeleg scrisorile persoanelor individuale, scrise de mână sau prin alte metode, transmise personal, prin curier sau prin poștă. În calitate de destinatar poate fi o singură persoană sau mai multe persoane (pluralitatea de destinatari). Noţiunea de ***corespondenţă*** semnifică *schimbul de scrisori între două persoane fizice sau juridice.* În funcţie de diferite criterii, corespondenţa poate fi clasificată după natura emitentului: a) corespondenţa de afaceri privată (sau de afaceri personală), întocmită de persoane fizice, care include solicitări de prospecte de vară, rezervarea unei camere de hotel,

abonamente la ziar; scrisori de felicitare, scrisori de mulţumire, telegrame etc.; b) corespondenţa oficială, întocmită de persoane juridice (cereri de ofertă, oferte, reclamaţii, somaţii, comenzi etc.).

La nivel internațional întâlnim încă o categorie de corespondență, cum ar fi poșta electronică. Generic vorbind, *poșta electronică* este o facilitate de comunicare oferită cetățenilor grație interconectării sistemelor informatice și cuplarea acestora la diferite tipuri de rețele care suportă protocoale necesare schimbului de mesaje electronice [4]. Potrivit Directivei 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice [7], *„poșta electronică"* înseamnă orice mesaj text, vocal, sau conținând sunete sau imagini trimise prin intermediul unei rețele de comunicații publice, care poate fi stocat în rețea sau în echipamentul terminal al destinatarului până la deschiderea sa de către acesta; *„comunicație"* înseamnă orice informație trimisă sau transmisă între un număr finit de părți prin intermediul unui serviciu public de comunicații electronice.

Termenul *„corespondență"* implică existența a cel puțin doi destinatari – nu credem că ar trebui să existe un astfel de consimțământ doar din partea uneia dintre aceste persoane. În opinia noastră, ambii participanți la corespondență sau la un eveniment privat trebuie să consimte la divulgarea sau la o altă formă de prelucrare a informațiilor confidențiale cu caracter privat.

Cu privire la definirea ***obiectului material/imaterial*** al infracțiunii, în literatura de specialitate se susține că acesta este *un bun în legătura cu care sau pentru care se săvârșește o infracțiune*, iar prejudiciul este cauzat nu obiectului material, ci obiectului juridic special al infracțiunii – obiectul material al infracțiunii nu suferă niciun prejudiciu [2, p.42-43]. Cauzarea reală a prejudiciului obiectului material al infracțiunii este absolut posibilă, însă nu este obligatorie [*Ibidem*].

Putem oare să recunoaștem astfel de date în calitate de obiect imaterial al infracțiunii? Dacă obiectul infracțiuni este un bun al lumii materiale, atunci în calitate de obiect material trebuie să fie recunoscut un purtător de informații: un document scris, CD-ul, banda magnetică etc. În realitate, însă, este posibilă încălcarea secretului corespondenței personale care nu este reflectată, înscrisă sau fixată în alt mod pe un dispozitiv material. Considerăm că prevederile de la alin.(1) art.178 CP RM presupun violarea dreptului la secretul corespondenței nu întotdeauna materializată. Prin urmare, datele ce constituie secret al corespondenței personale nu pot fi recunoscute drept obiect material, ci în calitate de obiect imaterial.

În acest perimetru de doctrină susținem ca oportună observația autorului S.Copețchi care constată că în alin.(1) art.178 CP RM se prevede răspunderea penală pentru *violarea dreptului la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei,* deși articolul are titulatura *„Violarea dreptului la secretul corespondenţei".* S.Copețchi subliniază: *„Pentru a intra în domeniul de aplicabilitate al art.8 CEDO, corespondența nu trebuie să aibă niciun caracter public: astfel, este exclusă, în principiu, corespondența comercială, administrativă sau publicitară, deoarece art.8 nu se aplică decât în cazul corespondenței private și în anumite circumstanțe profesionale. Mai mult, în doctrina Republicii Moldova se fac observații conform cărora violarea dreptului la secretul corespondenţei electronice scapă de sub incidența legii penale. Răspunderea penală este inaplicabilă în ipoteza violării dreptului la secretul corespondenței electronice întreținute prin e-mail sau pe altă cale ce nu presupune efectuarea de convorbiri telefonice sau expedierea de înștiințări telegrafice"* [8, p.117].

Din cele relatate autorul S.Copețchi observăm că în dispoziția articolului 178 CP RM rămân forme de corespondență desuete ce nu corespund realității sociale, cum ar fi telegramele, și, totodată, lipsesc forme de corespondență electronică (mesaje transmise prin e-mail, rețelele de socializare, spre exemplu – Facebook messenger, chat-uri, inclusiv Skype, Viber etc.). Se primește că dreptul la alte forme de corespondență care nu-și găsesc reflectare în dispoziția alin.(1) art.178 CP RM nu este protejat de norma juridico-penală ce incriminează fapta de violare a dreptului la secretul corespondenței. Astfel, autorul precitat consemnează că convorbirile telefonice și înștiințările telegrafice, comparativ cu scrisorile, telegramele, coletele și alte trimiteri poștale, constituie entități incorporale, motiv pentru care acestea formează categoria obiectelor imateriale [8, p.116]. Împărtășim observația autorului citat precum că Legea *comunicațiilor poștale* (17.03.2016) nu mai conține noțiunea *„telegramă".* S.Copețchi subliniază caracterul desuet, fapt ce a şi determinat inutilizarea acesteia în noua reglementare [8, p.116]. În astfel de ipoteză este inaplicabilă norma de la art.178 CP RM, deoarece norma extrapenală (de referință pentru cea de la art.178 CP RM) nu mai operează cu noțiunea *„telegramă".*

Latura obiectivă a infracțiunii prevăzute la alin.(1) art.178 CP RM este exprimată în *violarea dreptului la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei.*

Dex-ul oferă definiția violării, cum ar fi: încălcare, profanare, siluire. Termenul „violare" utilizat în textul legii are o semnificație largă, cuprinde mai multe *faze* și nu poate fi redus doar la divulgare propriu-zisă. Cu titlu de exemplu, pentru a se *„familiariza"*, făptuitorul trebuie să acceseze sau să obțină obiectele materiale anumite (scrisori, colete, telegrame etc.) și apoi să ia cunoștință de conținutul lor. Pentru a asculta o convorbire telefonică, el trebuie să se conecteze la acea linie telefonică și apoi să o asculte. Este puțin probabil că cineva este gata să susțină că retragerea și conectarea la linie nu fac parte din latura obiectivă a violării secretului corespondenței personale. Fără îndoială, încetarea activității infracționale la aceste etape, datorită unor circumstanțe care nu depind de voința făptuitorului, ar trebui să fie recunoscute ca pregătire la săvârșirea infracțiunii prevăzute la art.178 CP RM.

Cum ar trebui să calificăm fapta de oferire a oportunității unor persoane străine de a încălca secretul corespondenței săvârșită de către lucrătorii oficiului poștal sau ai centrului de comunicații, care nu se cunosc între ei și nu ascultă informațiile ce constituie secretul corespondenței personale, dar oferă altora o șansă să facă acest lucru? Spre exemplu, lucrătorul oficiului poștal trimite scrisoarea sigilată unei terțe părți, iar angajatul centrului de comunicații oferă acces la convorbirile telefonice de la al treilea telefon. Considerăm că în cazul în care persoana își folosește poziția oficială pentru a facilita ascultarea convorbirilor telefonice sau a asigura familiarizarea cu alte mesaje nu pentru sine, ci în interesul altor persoane, această persoană va răspunde pentru complicitatea la infracțiunea prevăzută la alin.(5) art.42 CP RM, lit.a) alin.(2) art.178 CP RM prin concurs cu fapta infracțională prevăzută la alin.(1) art.327 CP RM. Această soluție de încadrare juridico-penală nu poate fi reținută în cazul în care angajatul stației telefonice cunoștea despre intenția autorului și l-a asistat tehnic pe parcursul efectuării lucrărilor de conecare și de obținere a informației transmise prin rețeaua telefonică de telecomunicație – în astfel de cazuri persoana acționează în coautorat și nu în calitate de complice (lit.a) alin.(2) art.178 CP RM prin concurs cu fapta infracțională prevăzută la alin.(1) art.327 CP RM). Prin urmare, vom fi în prezența faptei de violare a corespondenței nu doar în cazul faptei de cunoaștere a conținutului informației confidențiale ce face obiectul imaterial al acestei infracțiuni, dar și în cazul obținerii accesului la rețelele de comunicații, inclusiv prin înlăturarea obstacolelor.

De menționat că noțiunea de *„violare"* este cu mult mai extinsă decât cea de *„divulgare"* cuprinzând și alte fapte care pot, în final, să prejudicieze în alt mod secretul corespondenței a unei alte persoane. Cea mai răspândită formă a violării, însă care nu este expres prevăzută de lege, este *„divulgarea"*. Practica denotă că securitatea informațiilor protejate de lege poate fi prejudiciată prin: *furtul* mijloacelor de informare în masă sau furtul informațiilor afișate prin intermediul acestora; *pierderea* suportului de informații; *scurgerea* de informații; *distrugerea* neautorizată a suportului de informații sau a informațiilor stocate pe acest suport; *denaturarea* informațiilor (modificări neautorizate, falsuri, fraudări); *blocarea* informațiilor; *divulgarea* informațiilor (distribuire, diseminare, destăinuire).

Divulgarea conținutului unei corespondențe, convorbiri sau înștiințări înseamnă relatarea, făcută chiar și unei singure persoane neîndreptățite, a conținutului unei corespondențe, convorbiri sau înștiințări efectuate între alte persoane. Nu are importanță modul în care făptuitorul a luat cunoștință de conținutul informației, legea imputându-i în toate cazurile să păstreze confidențialitatea asupra a celor aflate. Confidențialitatea informației este prevăzută de legislație.

Sustragerea corespondenței presupune *luarea ilegală și gratuită a purtătorilor materiali de informație ce conțin informații confidențiale protejate din posesia altuia (în cazul nostru, posesorul informațiilor confidențiale ce constituie secret al corespondenței), care a cauzat un prejudiciu patrimonial efectiv acestuia, săvârșită în scop de cupiditate.* La baza acestei definiții noi am pus definiția fundamentală a sustragerii propusă de autorul V.Stati. Astfel, în opinia acestui autor, *„în sensul legii, se consideră sustragere luarea ilegală şi gratuită a bunurilor mobile din posesia altuia, care a cauzat un prejudiciu patrimonial efectiv acestuia, săvârşită în scop de cupiditate"* [9, p.6], o astfel de definiție a sustragerii fiind chiar recomandată pentru reformularea explicației de la alin.(1) pct.2 al Hotărârii Plenului Curții Supreme de Justiție nr.23/2004 [10].

Sustragerea corespondenței nu întotdeauna este legată de obținerea acestor informații de către persoanele neautorizate. Uneori se întâmplă că sustragerea corespondenței este săvârșită de către colegii de la locul de muncă (persoane autorizate) din alte motive personale: invidie, ură, răzbunare. În astfel de cazuri, purtătorii

de corespondență se nimicesc de către persoanele care au săvârșit această sustragere. Putem concluziona că divulgarea corespondenței conduce, în mod inevitabil, la o scurgere, iar sustragerea și pierderea acesteia poate rezulta în scurgeri (cu alte cuvinte, există doar o probabilitate a unei scurgeri).

Termenul *„distrugere"* înseamnă orice tip de impact asupra corespondenței, în urma căruia se pierde posibilitatea utilizării ulterioare a acesteia de către oricine fără posibilitatea de a o recupera. Transferul informațiilor ce constituie corespondență pe un alt suport informatic nu este considerat, în contextul dreptului penal, faptă de distrugere a informației confidențiale, cu excepția cazurilor când, în urma acestor fapte, accesul utilizatorilor legitimi la informații a fost semnificativ împiedicat sau totalmente exclus. Distrugerea informațiilor nu poate fi manifestată în redenumirea fișierului în care este conținută, precum și în *„ștergerea automată"* a vechilor versiuni ale fișierelor.

Spre deosebire de fapta de pierdere, *distrugerea* corespondenței exclude posibilitatea ca alții să se familiarizeze cu conținutul acesteia. *Pierderea* corespondenței este ieșirea acesteia din posesia persoanei care are acces la secretul corespondenței. Pierderea poate fi completă sau parțială, irevocabilă sau temporară (în cazul blocării informațiilor), dar în orice caz este în detrimentul proprietarului acestei corespondențe. Pericolul survenirii unor urmări prejudiciabile încă nu înseamnă că această urmare nefastă a survenit sau va surveni în mod inevitabil. Astfel, purtătorul pierdut de informații confidențiale (cum ar fi, în cazul nostru, corespondența), pe de o parte, poate să nimerească la persoane neautorizate, sau, pe de altă parte, poate fi chiar blocat de camionul cu gunoi și, consecutiv, distrus. În astfel de cazuri nu se produc scurgeri de informații confidențiale.

Furtul mijloacelor de stocare, precum și *distrugerea* neautorizată a acestora sau doar a informațiilor stocale în ele, *destăinuirea* și *blocarea* informațiilor conduc la *pierderea* corespondenței.

Scurgerea informațiilor ce formează conținutul corespondenței conduce la *dezvăluirea acesteia*. În Partea specială a Codului penal se evită utilizarea termenului *„scurgeri de informații confidențiale"*, acesta fiind înlocuit sau identificat cu termenii *„dezvăluire"* și *„divulgare"*. Indiscutabil, scurgerea se produce atunci când are loc divulgarea (distribuirea neautorizată) a informațiilor confidențiale, dar, în opinia noastră, nu se limitează la aceasta, fiind acoperite fapte de *pierdere* și *furt*.

Deseori, cum denotă practica judiciară a Republicii Moldova, violarea dreptului la secretul corespondenței nu se săvârșește de sine stătător, ci cu un scop special și în cadrul unor activități abuzive sau excesive în procesul de îndeplinire a obligațiilor de serviciu. Prin urmare, fapta de violare a secretului corespondenței este calificată prin concurs cu alte fapte, spre exemplu – cu excesul de putere sau depăşirea atribuţiilor de serviciu (art.328 CP RM), fiind săvârșită în detrimentul intereselor servicilui public. Întru confirmarea celor expuse aducem un caz din practica judiciară a Republicii Moldova [11]: Prin sentința Judecătoriei Militare mun. Chişinău din 26 decembrie 2012, Ţ.R. a fost condamnat pentru săvârşirea infracţiunilor prevăzute la lit.a) alin.(2) art.178 şi la alin.(1) art.328 CP RM. Instanța a stabilit următoarele: *Ţ.R., exercitând funcţia de şef al Direcţiei XXX SIS, în perioada 11.02.2008 – 02.10.2009, având obligaţia de a asigura tehnic, în incinta sediului SIS, interceptarea convorbirilor telefonice, controlul comunicărilor telegrafice şi al altor comunicări prin intermediul reţelelor electronice, cu utilizarea mijloacelor tehnice speciale, folosind situaţia de serviciu, încălcând prevederile legislaţiei în vigoare, inclusiv fără a avea spre executare încheierea judecătorului de instrucţie privind autorizarea interceptării convorbirilor telefonice ale fostului colaborator al SIS A.V., a ordonat împuternicitului operativ superior G.O. efectuarea asigurării tehnice a interceptării convorbirilor telefonice ale acestuia prin activarea pentru interceptarea numărului de telefon 0XXXXXXX6, ultimul executând ordinul superiorului său Ţ.R., despre care G.O. nu ştia că este ilegal. Astfel, G.O. a asigurat tehnic interceptarea convorbirilor telefonice în perioada de la 03.11.2008 şi până la 06.04.2009 de pe numărul de telefon 0XXXXXXX6 utilizat de A.V., încălcând astfel dreptul acestuia la secretul convorbirilor telefonice, fără a înregistra în perioada indicată acest fapt în registrul de evidenţă a interceptărilor convorbirilor telefonice.*

Într-un alt caz [12], prin sentinţa Judecătoriei Grigoriopol, cu sediul în mun. Chişinău, din 26 mai 2011, C.S. a fost achitat de sub învinuirea de săvârşirea infracţiunii prevăzute la lit.a) alin.(2) art.178, alin.(1) art.327, alin.(1) art.328 şi alin.(1) art.332 Cod penal, din motiv că fapta inculpatului nu întruneşte elementele infracţiunii. Instanța de fond a stabilit următoarele: *C.S. a fost învinuit de către organul de urmărire penală pentru faptul că, deţinând funcţia de inspector superior în Secţia Misiuni Speciale în Direcţia Misiuni Speciale a MAI, la 27 mai 2009, aflându-se în biroul de serviciu, a emis ordonanţa cu nr.532 ss despre pornirea dosarului de prelucrare operativă a lui S.Q. pe faptul că în mun.Chişinău activează un grup de*

persoane, condus de S.Q, care organizează migraţiunea ilegală a cetăţenilor Republicii Moldova în spaţiul „Schengen" cu folosirea actelor false. În temeiul prezentei ordonanţe a fost pornit dosarul de prelucrare operativă cu numărul XXXXXXX, în cadrul căruia au fost luaţi la evidenţă operativă cet.S.Q. şi cet.M.N. La 10 iunie 2009 C.S. a întocmit extrasul din nota agent-turistică nr.385 ss în care a indicat precum că la întâlnirea ordinară a colaboratorului secret a comunicat că liderii grupării criminale folosesc în schemele lor următoarele telefoane mobile: S.Q. – 0XXXXXXX4, 0XXXXXXX2, 0XXXXXXX3, 0XXXXXXX5 şi M.N. – 0XXXXXXX7, 0XXXXXXX0, 0XXXXXXX9, 0XXXXXXX6, 0XXXXXXX1, 0XXXXXXX8. În temeiul acestei note agent-turistice, S.Q, folosindu-se de dreptul de a dispune interceptarea convorbirilor telefonice, indicând date vădit incorecte, a întocmit ordonanţa cu nr.584 ss, *privind interceptarea convorbirilor telefonice şi a altor convorbiri, prin care a fost dispusă interceptarea convorbirilor telefonice ale posesorilor altor numere de telefon* [12].

Violarea corespondenței personale poate fi exprimată prin diverse ***acțiuni***: prin deschiderea ilegală a scrisorilor și a altor corespondențe pentru a se familiariza cu conținutul lor; prin dezvăluirea conținutului corespondenței unor alte persoane etc. [2, p.13-14].

Distingem trei situații de calificare a violării secretului corespondenței, după cum urmează:

- Conform regulii generale, când încălcarea inviolabilității vieții personale are loc prin violarea secretuuli corespondenței, cele săvârșite sunt încadrate în prevederile de la art.178 CP RM, deoarece norma juridico-penală prevăzută la alin.(1) art.177 CP RM, este una generală, în sensul culegerii, față de norma prevăzută la alin.(1) art.178 CP RM, care este specială. Alegerea respectivă este determinată de utilizarea culegerii „calificate", specifice. Norma prevăzută la alin.(1) art.178 CP RM conține prevederi speciale în raport cu norma generală (art.177 CP RM) și nu poate fi aplicată prin concurs, iar în cazul concurenței între normă generală și cea specială va fi aplicată norma specială. Prin urmare, opinia autorului rus I.R. Divaeva [13, p.88], conform căreia atentarea la inviolabilitatea vieții personale exprimată în culegerea datelor, spre exemplu prin violarea secretului corespondenței, urmează a fi calificată prin concurs (cu referire la legislația Republicii Moldova – art.177 și art.178 CP RM – *n.a.*), devine irelevantă.
- Concursul normei prevăzute la alin.(1) art.177 CP RM și la alin.(1) art.178 CP RM va fi posibil în cazul în care urmează a fi încadrată o altă faptă infracțională prevăzută la alin.(1) art.177 CP RM și neacoperită de alin.(1) art.178 CP RM, spre exemplu – în cazul în care informațiile ce constituie secret personal sunt culese prin metoda violării secretului corespondenței, iar ulterior răspândite.
- În cazul în care datele despre viața privată a unei alte persoane sunt acumulate/colectate/culese prin ascultarea conversațiilor care nu se întreţin la telefon sau printr-un alt mijloc de comunicare, în special prin intermediul comunicării personale directe verbale și înregistrarea acestora, spre exemplu – prin mijloace de fixare audio aflate pe haina făptuitorului, cele comise urmează a fi calificate doar în baza art.177 CP RM fără vreo referință la prevederile de la art.178 CP RM.

Dacă secretul corespondenței personale este încălcat, iar apoi sunt dezvăluite informațiile ce constituie secret personal sau familial, atunci cele comise vor fi calificate prin concurs (art.177 și art.178 CP RM). În cazul în care informațiile ce constituie corespondența sunt protejate într-un regim de secret special, cele comise urmează a fi calificate în baza art.178 CP RM prin concurs cu altă normă specială care prevede răspunderea penală pentru încălcarea inviolabilității și confidențialității datelor confidențiale păstrate în regim secret.

Observăm că, în sensul alin.(1) art.178 CP RM, nu este clar dacă *distrugerea* corespondenței poate fi privită sau nu ca formă a violării dreptului la secretul corespondenței. Totodată, pentru a aduce claritate și o mai mare previzibiltate a legii penale, propunem concretizarea dispoziției de la alin.(1) art.178 CP RM prin introducerea sintagmei *„distrugerea corespondenței"*, care, în opinia noastră, este cu mult mai gravă și prejudiciabilă decât simpla citire a mesajului.

În opinia noastră, violarea dreptului la secretul corespondenței cuprinde și depozitarea ulterioară a scrisorilor sau a altor purtători de aceleași informații protejate de lege și, prin urmare, se califică doar în baza alin.(1) art.178 CP RM.

O altă problemă pe care o sesizăm din analiza conținutului art.178 CP RM este lipsa protecției speciale a secretului profesional care este răspândit prin violarea secretului corespondenței. În același timp, spre deosebire de legea penală a Republicii Moldova, în conformitate cu alin.(3) art.302 din Codul penal al României, constituie infracțiune faptele prevăzute în alin. (1) şi alin. (2) care au fost săvârşite de un *funcţionar public care are obligaţia legală de a respecta secretul profesional şi confidenţialitatea informaţiilor la care are acces*.

În scopul îmbunătățirii cadrului incriminator și întru asigurarea protecției juridico-penale a secretului profesional, propunem completarea alin.(2) art.178 CP RM cu lit.d) având următorul text: *„fapta prevăzută la alin.(1) sau la alin.(2) săvârşită de* către *persoana care are obligaţia legală de a respecta secretul profesional şi confidenţialitatea informaţiilor la care are acces"*.

În același timp, fapta infracțională se consideră *consumată* din momentul în care informația confidențială devine cunoscută terților prin accesul ilegal la aceasta. Totodată, activitatea de stocare/depozitare/păstrare este asociată doar cu continuarea încălcării drepturilor personale la corespondență și nu sunt obligatorii pentru calificare. În acest perimetru de cercetare, suntem de acord cu autorul rus D.V. Bușkov, care pledează pentru introducerea unei circumstanțe agravante, cum ar fi obținerea de către terț a informațiilor confidențiale ce fac parte din secretul corespondenței unei alte persoane în urma încălcării dreptului la secretul corespondenței [2, p.14].

Mijloacele de săvârşire a infracţiunii includ, de exemplu, înregistrări video și audio, film și fotografie, precum și alte mijloace tehnice care nu prejudiciază viața și sănătatea individului și mediul. De remarcat că, în opinia legiuitorului, mijloacele menționate mai sus trebuie înțelese doar ca mijloace tehnice care au un scop funcțional specific – *achiziţionarea/ dobândirea* de informații ascunse. D.V. Bușkov susține că *cunoaşterea informaţiei confidenţiale prin fapta de primire neautorizată în urma divulgării de către o altă persoană trebuie considerată o circumstanţă agravantă* [2, p.103]. De specificat că folosirea poziției oficiale de către persoană ca metoda de săvârșire a acestei infracțiuni crește în mod semnificativ pericolul public al infracțiunii. Pe baza celor de mai sus, o încălcare a secretului corespondenței personale trebuie înțeleasă ca o acțiune sau o omisiune comisă în vreun fel care ar aduce atingere interesului supus protecției de dreptul penal [2, p.104].

Care ar fi încădrarea juridică a faptei de divulgare a datelor personale transmise prin mesaje electronice?

Răspunsul este unicul posibil: secretul corespondenței electronice, în conformitate cu legea penală actuală a Republicii Moldova, nu constituie obiectul imaterial al infracțiunii prevăzute la alin.(1) art.178 CP RM, iar divulgarea acestuia va fi încadrată potrivit prevederilor unei norme juridico-penale generale care asigură protecția juridico-penală a secretului primar care este transmis prin corespondență (cu titlu de exemplu, alin.(1) art.177 CP RM), sub forma culegerii. Spre exemplu, în cazul în care este încălcat secretul corespondenței personale (divulgarea conversației personale, distribuirea pozelor sau a secvențelor video cu caracter personal fără consimțământul persoanei) cele săvârșite urmează a fi calificate în baza art.177 CP RM (Încălcarea inviolabilității vieții personale) sub forma de *răspândire* și, în funcție de împrejurările cauzei, în baza alin.(1) art.259 CP RM (Accesul ilegal la informaţia computerizată), după caz, prin concurs cu art.260[1] CP RM (Interceptarea ilegală a unei transmisii de date informatice). Devine evident că Partea specială a Codului penal al Republicii Moldova oferă protecție juridico-penală datelor confidențiale cu caracter personal în regim de secret primar în sensul normei juridico-penale prevăzute la alin.(1) art.177 CP RM. Acest răspuns este relevant pentru informațiile cu privire la viață privată, cu condiția că ele nu sunt acoperite de alte regimuri secundare, cum ar fi, spre exemplu, secretul de serviciu, secretul bancar etc.

În același timp, încălcarea secretului corespondenței ce a constat în divulgarea secretului adopției prin mijloace electronice (spre exemplu, luarea cunoștinței de conținutul mesajului electronic privat pe Messenger Facebook) se va încădra în fapta prevăzută la alin.(1) art.204 CP RM și, după caz, prin concurs cu alin.(1) art.259 și art.260[1] CP RM. Această soluție de încădrare juridico-penală este una corectă, deoarece secretul adopției este tipul special al secretului personal sau familial și, pe cale consecință, norma juridico-penală prevăzută la alin.(1) art.204 CP RM este una specială în comparație cu norma prevăzută la alin.(1) art.177 CP RM.

În cazul în care datele personale confidențiale sunt păstrate în regimul secundar de secret bancar sau comercial, încălcarea secretului corespondenței (spre exemplu, accesul neautorizat la informaţia computerizată ce constituie secret bancar sau comercial și interceptarea ilegală a transmisiei de date informatice confidențiale ce constituie secret bancar sau comercial), se va califica prin concurs de infracțiuni prevăzute la art.245[10] CP RM (Obţinerea ilegală şi/sau divulgarea informaţiilor ce constituie secret comercial sau bancar), la alin.(1) art.259 și la art.260[1] CP RM.

Într-un alt perimetru de cercetare, spre deosebire de prevederile art.178 CP RM (Violarea secretului corespondenței), infracțiunile informatice au în calitate de *obiect juridic prinicipal* integritatea, confidențialitatea și securitatea informației computerizate. O protecție deosebită dobândesc datele informatice protejate

de lege, adică categoriile speciale de informație computerizată. Deși inviolabilitatea vieții private nu este prevăzută în calitate de obiect juridic principal, ni se pare suficientă împrejurarea că astfel de valori sociale pot constitui obiectul juridic secundar. Categoria *„datele informatice cu acces limitat"*, în sensul art.260[2] CP RM, fiind o categorie mai extinsă, acoperă perfect datele informatice ce constituie secret profesional, deoarece informațiile confidențiale asigurate prin regim de secret profesional sunt date cu acces limitat.

Considerăm oportun să identificăm câteva soluții de calificare a accesului ilegal la informația computerizată ce constituie secret profesional în lumina art. 259 CP RM. Astfel, în conformitate cu alin.(1) art.259 CP RM, constituie infracțiunie *accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice şi dacă a cauzat daune în proporţii mari*.

În opinia noastră, accesul ilegal la informația computerizată ce constituie secret profesional va constitui infracțiune în sensul lit.d) alin.(2) art.259 CP RM doar în cazul în care sunt respectate câteva condiții obligatorii: 1) informația este computerizată; 2) subiectul faptei infacționale este o persoană neautorizată; 3) accesul este însoțit de alte acțiuni; 4) accesul a cauzat daune în proporţii mari; 5) obiectul imaterial al faptei de acces ilegal la informația computerizată îl constituie informația protejată de lege.

Sintagma *„informație protejată de lege"* va include și o categorie specială de informații protejate de lege, cum ar fi secretul profesional. De reținut că informația confidențială cu privire la viața privată a persoanei, protejată atât în regim de secret primar, cât și în regim de sercret secundar (spre exemplu, profesional), fiind informație protejată de lege, constituie obiectul imaterial al infracțiunii prevăzute la lit.g) alin.(2) art. 259 CP RM.

În sensul alin.(1) art.259 CP RM, accesul reprezintă un proces de asigurare a posibilității de a implementa un act de familiarizare și (sau) manipulare a informațiilor confidențiale, de exemplu: citirea de pe monitor a informațiilor ce nu-i aparțin subiectului, persoana neavând dreptul să facă acest lucru. Dacă o persoană obține accesul neautorizat fără a purcede la distrugere, blocare, modificare sau copiere a informațiilor, la scoaterea din funcțiune a calculatorului, a sistemului informatic sau a rețelei acestora, un astfel de act nu va atrage răspunderea penală.

Accesul la informații confidențiale presupune identificarea și cunoașterea de către o persoană autorizată a unei persoane căreia îi aparțin astfel de date. Acțiunile de acces includ: primirea, trimiterea, revizuirea, reînnoirea, înlocuirea, înregistrarea, controlul, execercitarea, supravegherea calității executării, întreținerea bazelor de date, editarea, stocarea și utilizarea. *Utilizarea datelor cu caracter personal* reprezintă o acțiune sau o serie de acțiuni cu acestea, efectuate de către un operator pentru a lua decizii sau acțiuni de altă natură ce dau naștere unor consecințe juridice în legătură cu subiectul datelor cu caracter personal sau cu alte persoane sau care afectează în alt mod drepturile și libertățile acestui subiect sau ale altor persoane. Conform articolului 4 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 [14], *„creare de profiluri"* înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia.

Accesul la informații confidențiale este ilegal în două cazuri: persoana nu are dreptul de a accesa aceste informații (este o persoană neautorizată); persoana are dreptul de a accesa aceste informații, însă accesul este executat fără respectarea procedurii stabilite, normele de protecție a acestor informații fiind încălcate [15, p.112]. *Accesul ilegal la informații protejate* poate fi privit ca un proces de asigurare a posibilității de a săvârși un act de familiarizare și (sau) manipulare a informațiilor confidențiale. Pe de altă parte, accesul poate fi privit ca rezultat al acțiunilor care vizează familiarizarea și/sau manipularea informațiilor confidențiale, de exemplu: citirea de pe ecranul computerului a informațiilor relevante de către un subiect neautorizat.

Accesul este considerat ilegal, în sensul art.259 CP RM, dacă este *însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice.*

Distrugerea informațiilor protejate de lege presupune un impact specific asupra acestor date protejate în urma căruia purtătorii de informații sunt nimiciți (înlăturați) fizic, fie, în general, încetează să existe în orice formă materializată accesibilă pentru percepție și fixare sau sunt supuse unei astfel de modificări, în care cele mai semnificative componente ale informațiilor din purtător nu sunt în stare să reflecte conținutul informațiilor originale în întregime. Transferul simultan al informațiilor pe un alt suport informatic nu este considerat, în contextul dreptului penal, un act de distrugere a informației digitale, cu excepția cazului în care ca urmare a acestor acțiuni accesul utilizatorilor legitimi la informații nu a fost semnificativ împiedicat sau exclus. *Distrugerea informației* nu înseamnă redenumirea fișierului în care ea se conține, ci și *„dispariția"* automată a versiunilor vechi ale fișierelor de către ultima dată în timp. Termenul *„distrugere"* înseamnă un tip de impact asupra informațiilor pe calculator, în urma căruia se pierde posibilitatea utilizării ulterioare de către oricine.

Modificarea informației înseamnă o schimbare a conținutului lor în comparație cu informațiile care au fost inițial la dispoziția proprietarului sau a utilizatorului legitim. Vorbind despre modificare, trebuie subliniat faptul că aceasta este o acțiune de schimbare a valorii informațiilor în direcția dorită (specificată). Cel mai important element din definiția *„modificării"* este direcția schimbării informațiilor. Dacă nu se concentrează acțiunile efectuate, atunci aceasta nu mai sunt o modificare, ci distrugerea informațiilor. În informatică, termenul *„modificare"* este folosit pentru a desemna modificări care nu schimbă esența unui obiect. Astfel de acțiuni privind informația din calculator, spre exemplu, sunt direct legate de noțiunile de *„adaptare"* și *„decompilare"* a programelor care există deja în legislația actuală. În conformitate cu prevederile art.3 din Legea Republicii Moldova *cu privire la schimbul de date și interoperabiltate,* nr.142 din 19.07.2018 [16], *adaptarea datelor* reprezintă un procedeu tehnologic de transformare, care include formatarea, agregarea, dezagregarea, consolidarea și segregarea datelor disponibile sau transmise prin intermediul platformei de interoperabilitate, fără denaturarea acestora, cu scopul eficientizării procesului de schimb și/sau de prelucrare a datelor.

Blocarea informațiilor reprezintă un set de acțiuni sau o singură acțiune ce creează o dificultate artificială totală sau parțială (utilizarea informațiilor devenind imposibilă sau substanțial dificilă) în accesare la informații de către utilizatori; astfel de acțiuni nu sunt legate de distrugerea acestor informații. Conceptul de blocare a informațiilor coincide în mare măsură cu cel de denaturare a informațiilor și diferă numai prin faptul că informațiile de control nu sunt supuse modificării. De exemplu, pentru a bloca accesul unui utilizator legal la bazele de date, este necesar să se opereze modificări în fișierele sistemului administratorului de rețea, însăși baza de date protejată nefiind supusă cărorva modificări.

Conceptele *„modificare ", „distrugere", „blocare"* sunt strâns legate între ele, deoarece la nivelul fizic al reprezentării informației este posibil din punct de vedere tehnic să se efectueze doar trei acțiuni – *citirea, scrierea* și *distrugerea* purtătorului însuși. Datorită cunoștințelor avansate referitoare la procesele ce apar în calculator și în rețelele acestuia, precum și ținând cont de nevoia de a obține cunoștințe speciale, faptele de copiere, modificare, blocare și distrugere a informațiilor ar trebui să fie demonstrate și stabilite prin expertiză tehnică specializată pe calculator. Capacitatea utilizatorului de a recupera informațiile distruse folosind instrumente software sau de a obține aceste informații de la un alt utilizator nu scutește făptuitorul de răspundere penală.

Copierea informațiilor – există numeroase opinii cu privire la interpretarea acestui concept. De exemplu, unii autori consideră că copierea informațiilor din calculator este o repetare și o fixare stabilă a acestora în calculator sau pe alte suporturi media. *Copierea informațiilor* se poate realiza prin înregistrarea conținutui în memoria internă a unui computer, imprimarea acestuia, copierea manuală a informațiilor din calculator (de exemplu, rescrierea textului de pe ecranul unui calculator pe o foaie de hârtie), prin fotografierea textului de pe ecranul dispozitivului. *Reproducerea informațiilor* trebuie distinsă de *copierea informațiilor* din calculator. Copierea poate fi înțeleasă doar ca acțiuni intenționate pentru a crea o copie a unui fișier pe orice mediu. *„Copierea informațiilor"* înseamnă o astfel de acțiune neautorizată de către proprietarul legal (proprietar, utilizator) a informațiilor și (sau) încălcarea legii privind utilizarea (deținerea, eliminarea) în rezultatul căreia apare o altă copie (sau mai multe) a informațiilor originale, reprezentând repetarea exactă a acesteia (duplicarea originală a informațiilor).

Accesul ilegal la informația computerizată săvârșit în coautorat va fi încadrat în baza prevederilor de la lit.b) alin.(2) art.259 CP RM, însă înlăturarea de obstacole fizice, digitale și de altă natură cu scopul de a

ușura accesul ilegal la informația computerizată a unei persoane străine va constitui, după caz, complicitate (alin.(5) art.42 CP RM) la infracțiunea prevăzută la alin.(1) art.259 CP RM, iar coautoratul, în sensul lit.b) alin.(2) art.259 CP RM, va lipsi.

Alături de accesul ilegal la informația computerizată, legea penală a Republicii Moldova incriminează și fapta de *interceptare ilegală a unei transmisii de date informatice* (inclusiv a unei emisii electronice) care nu sunt publice şi care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic. În acest mod, pentru a reține fapta infracțională prevăzută la art.260[1] CP RM, în acțiunile făptuitorului este necesar să stabilim prezența următoarelor condiții obligatorii ce se impun reieșind din conținutul dispoziției art.260[1] CP RM: interceptarea este ilegală; este interceptată o transmisie de date informatice; datele informatice nu sunt publice; datele informatice sunt destinate unui sistem informatic. Informațiile confidențiale asigurate în regim de secret profesional se acoperă de sintagma *„date informatice ce nu sunt publice"*.

Luând în considerare că interceptarea informației confidențiale computerizate constituie o faptă infracțională de sine stătătoare prevăzută la art.260[1] CP RM, accesul ilegal la informația computerizată protejată de lege, însoțit de interceptarea informației computerizate protejate de lege, urmează a fi calificat prin concurs de infracțiuni prevăzute la art.260[1] CP RM și la lit.g) alin.(2) art.259 CP RM. Totodată, în cazul faptei infracționale prevăzute la lit.g) alin.(2) art.259 CP RM pot avea loc etapele activității infracționale atât sub forma pregătirii, cât și sub forma tentativei. Deoarece fapta de acces ilegal nu se acoperă de latura obiectivă a interceptării în sensul art.260[1] CP RM, fapta de acces ilegal la informația computerizată protejată de lege, în scopul de a o intercepta, urmează a fi calificată ca faptă consumată prevăzută la lit.g) alin.(2) art.259 CP RM și ca pregătire la infracțiunea de interceptare ilegală a unei transmisii de date informatice (art.260[1] și art.26 CP RM). În cazul unui acces ilegal la informația computerizată protejată și al unei interceptări ilegale a unei transmisii de date informatice eșuate din cauza unor împrejurări obiective ce nu depind de voința făptuitorului, în acțiunile acestuia se va reține concursul de infracțiuni prevăzute la lit.g) alin.(2) art.259 CP RM și tentativa pentru infracțiunea de interceptare ilegală a unei transmisii de date informatice (art.260[1] și art.27 CP RM).

Informații confidențiale asigurate prin regim de secret profesional constituie datele informatice cu acces limitat, iar dobândirea, comercializarea sau punerea la dispoziţie a acestora sub orice formă va constitui fapta infracțională prevăzută la art.260[2] CP RM (Alterarea integrităţii datelor informatice ţinute într-un sistem informatic) – *dobândirea, comercializarea sau punerea la dispoziţie, sub orice formă*. Totodată, potrivit prevederilor de la art.261 CP RM (Încălcarea regulilor de securitate a sistemului informatic), constituie infracțiune *încălcarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic, prevăzute în conformitate cu statutul informaţiei sau gradul ei de protecţie, dacă această acţiune a contribuit la însuşirea, denaturarea sau la distrugerea informaţiei ori a provocat alte urmări grave*. Astfel, informația confidențială ce se asigură prin regim de secret profesional va constitui obiectul imaterial al infracțiunii prevăzute la art.261 CP RM. Încălcarea următoarelor reguli constituie infracțiune, în sensul art.261 CP RM: *a regulilor de colectare, prelucrare, păstrare, difuzare și de repartizare a informației.* Încălcarea unor astfel de reguli va constitui infracțiune doar în cazul în care ea a contribuit la însușirea, denaturarea sau la distrugerea informației ori a provocat alte urmări grave.

Însușirea presupune obținerea informației, *denaturarea* constituie modificarea esențială a informației, iar *distrugerea* informației desemnează nimicirea acesteia, pe când reconstruirea ei devine imposibilă sau, din punct de vedere tehnic sau economic, irezonabilă.

Concluzii și recomandări

− Când încălcarea inviolabilității vieții personale are loc prin violarea secretului corespondenței, cele săvârșite sunt încadrate în prevederile de la art.178 CP RM, deoarece norma juridico-penală prevăzută la alin.(1) art.177 CP RM este una generală, în sensul culegerii, față de norma prevăzută la alin.(1) art.178 CP RM care este specială. Alegerea respectivă este determinată de utilizarea culegerii *„calificate"*, specifice. Norma prevăzută la alin.(1) art.178 CP RM conține prevederi speciale în raport cu norma generală (art.177 CP RM) și nu poate fi aplicată prin concurs, iar în cazul concurenței între norma generală și cea specială, va fi aplicată norma specială.

− Concursul normei prevăzute la alin.(1) art.177 CP RM și la alin.(1) art.178 CP RM va fi posibil doar în cazul în care urmează a fi încadrată o altă faptă infracțională prevăzută la alin.(1) art.177 CP RM și

neacoperită de alin.(1) art.178 CP RM, spre exemplu în cazul în care informațiile ce constituie secret personal sunt *culese* prin metoda violării secretului corespondenței, iar ulterior *răspândite*.

– În cazul în care datele despre viața privată a unei alte persoane sunt acumulate/colectate/culese prin ascultarea conversațiilor care nu se întreţin la telefon sau printr-un alt mijloc de comunicare, în special prin intermediul comunicării personale directe verbale și prin înregistrarea concomitentă a acestora (spre exemplu, prin mijloace de fixare audio aflate pe haina făptuitorului), cele comise urmează a fi calificate doar în baza art.177 CP RM fără vreo referință la prevederile art.178 CP RM.

– Dacă secretul corespondenței personale este încălcat, iar apoi sunt dezvăluite informațiile ce constituie secret personal sau familial, atunci cele comise vor fi calificate prin concurs (art.177 și art.178 CP RM). În cazul în care informațiile ce constituie corespondența sunt protejate într-un regim de secret special, atunci cele comise urmează a fi calificate în baza art.178 CP RM prin concurs cu altă normă specială care prevede răspunderea penală pentru încălcarea inviolabilității și confidențialității datelor confidențiale păstrate în regim secret.

– În cazul în care persoana își folosește poziția oficială pentru a facilita ascultarea convorbirilor telefonice sau a asigura familiarizarea cu alte mesaje nu pentru sine, ci în interesul altor persoane, această persoană va răspunde pentru complicitate la infracțiunea prevăzută la alin.(5) art.42 CP RM, lit.a) alin.(2) art.178 CP RM prin concurs cu fapta infracțională prevăzută la alin.(1) art.327 CP RM. Această soluție de încadrare juridico-penală nu poate fi reținută în cazul în care angajatul stației telefonice cunoștea despre intenția autorului și l-a asistat tehnic pe parcursul efectuării lucrărilor de conectare și de obținere a informației transmise prin rețeaua telefonică de telecomunicație – în astfel de cazuri persoana acționează în coautorat și nu în calitate de complice (lit.a) alin.(2) art.178 CP RM prin concurs cu fapta infracțională prevăzută la alin.(1) art.327 CP RM). Prin urmare, vom fi în prezența faptei de violare a corespondenței nu doar în cazul faptei de cunoaștere a conținutului informației confidențiale ce face obiectul imaterial al acestei infracțiuni, dar și în cazul obținerii accesului la rețelele de comunicații, inclusiv prin înlăturarea obstacolelor.

– O altă problemă pe care o sesizăm din analiza conținutului art.178 CP RM este lipsa protecției speciale a secretului profesional care este răspândit prin violarea secretului corespondenței. În același timp, spre deosebire de legea penală a Republicii Moldova, în conformitate cu alin(3) art.302 din Codul penal al României, constituie infracțiune faptele prevăzute în alin.(1) şi alin.(2) care au fost săvârşite de un *funcţionar public care are obligaţia legală de a respecta secretul profesional şi confidenţialitatea informaţiilor la care are acces*. În scopul îmbunătățirii cadrului incriminator și întru asigurarea protecției juridico-penale a secretului profesional, propunem completarea alin.(2) art.178 CP RM cu lit.d) având următorul text: *„fapta prevăzută la alin.(1) sau alin.(2) săvârşită de* către *persoana care are obligaţia legală de a respecta secretul profesional şi confidenţialitatea informaţiilor la care are acces"*.

– În cazul în care este încălcat secretul corespondenței personale (divulgarea conversației personale, distribuirea pozelor sau a secvențelor video cu caracter personal fără consimțământul persoanei), cele săvârșite urmează a fi calificate în baza art.177 CP RM (Încălcarea inviolabilității vieții personale) sub forma de *răspândire* și, în funcție de împrejurările cauzei, în baza alin.(1) art.259 CP RM (Accesul ilegal la informaţia computerizată), după caz, prin concurs cu art.260[1] CP RM (Interceptarea ilegală a unei transmisii de date informatice). Devine evident că Partea specială a Codului penal al Republicii Moldova oferă protecția juridico-penală a datelor confidențiale cu caracter personal în regim de secret primar în sensul normei juridico-penale prevăzute la alin.(1) art.177 CP RM. Acest răspuns este relevant pentru informațiile cu privire la viața privată, cu condiția că ele nu sunt acoperite de alte regimuri secundare, cum ar fi, spre exemplu, secretul de serviciu, secretul bancar etc.

– În cazul în care datele personale confidențiale sunt păstrate în regimul secundar de secret bancar sau comercial, încălcarea secretului corespondenței (spre exemplu, accesul neautorizat la informaţia computerizată ce constituie secret bancar sau comercial și interceptarea ilegală a transmisiei de date informatice confidențiale ce constituie secret bancar sau comercial) se va califica prin concurs de infracțiuni prevăzute la art.245[10] CP RM (Obţinerea ilegală şi/sau divulgarea informaţiilor ce constituie secret comercial sau bancar), la alin.(1) art.259 și la art.260[1] CP RM.

– Sintagma *„informaţie protejată de lege"* (lit.g) alin.(2) art. 259 CP RM) va include și o categorie specială de date confidențiale protejate, cum ar fi secretul profesional.

– Accesul ilegal la informația computerizată protejată de lege, însoțit de interceptarea informației computerizate protejate de lege, urmează a fi calificat prin concurs de infracțiuni prevăzute la art.260[1] CP RM și la lit.g) alin.(2) art.259 CP RM.

– Deoarece fapta de acces ilegal nu se acoperă de latura obiectivă a interceptării în sensul art.260[1] CP RM, fapta de acces ilegal la informația computerizată protejată de lege, în scopul de a o intercepta, urmează a fi calificată ca faptă consumată prevăzută la lit.g) alin.(2) art.259 CP RM CP RM și ca pregătire la infracțiunea de interceptare ilegală a unei transmisii de date informatice (art.260[1] CP RM și art.26 CP RM).

– În cazul unui acces ilegal la informația computerizată protejată și al unei interceptări ilegale a unei transmisii de date informatice eșuate din cauza unor împrejurări obiective ce nu depind de voința făptuitorului, în acțiunile acestuia se va reține concursul de infracțiuni prevăzute la lit.g) alin.(2) art.259 CP RM și tentativa pentru infracțiunea de interceptare ilegală a unei transmisii de date informatice (art.260[1] și art.27 CP RM).

– Legea penală moldavă ar trebui să fie revizuită, drept exemplu al tehnicii legislative servind legea penală română, în special prevederile de la alin.(1)-(6) art.302 CP Rom. Legiuitorul moldav folosește sintagma ***„dreptul la secretul corespondenței"*** în denumirea articolului art.178 CP RM și sintagma „*dreptul la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice*" în conținutul alin.(1) din acest articol. Compărând aceste sintagme, devine evident că ele nu pot fi considerate egale și identice după sens: denumirea articolului se referă la dreptul la secretul oricărei forme de corespondență, iar dispoziția de la alin.(1) art.178 CP RM cuprinde doar dreptul la o listă restrictivă de corespondență – *scrisori, telegrame, colete şi alte trimiteri poştale, convorbiri telefonice şi înştiinţări telegrafice*".

– *Activitatea de prelucrare a datelor cu caracter personal* este cu mult mai vastă decât acțiunile incriminate de legea penală a Republicii Moldova.

– Comparând ambele definiții (cea din Regulamentul (CE) nr.45/2001 și din legislația română, pe de o parte, și cea adoptată de legislația extrapenală a Republicii Moldova (Legea Republicii Moldova *cu privire la protecția datelor cu caracter personal,* nr.17-XVI din 15.02.2007 [17]), pe de altă parte), devine evident că acțiunile de *alăturare, combinare* și *ștergere* nu și-au găsit oglindire în Legea Republicii Moldova nr.17-XVI/2007. Totodată, în opinia noastră, acțiunile de alăturare și combinare se vor include perfect în acțiunea de utilizare, unde alăturarea și combinarea ar constitui forme de sine stătătoare ale utilizării.

– Rămâne nesoluționată reflectarea în textul normei internaționale și în al celei din România a acțiunii de *acordare a accesului* care este expres prevăzută de Legea Republicii Moldova nr.17-XVI/2007. În opinia noastră, acțiunea de *precizare* ar fi realizată doar prin acces la astfel de date protejate și ar trebui să fie percepută și la nivel internațional.

Referințe:

1. Legea Republicii Moldova privind comunicaţiilor electronice, nr.241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2007, nr.51-54.
2. БУШКОВ, Д.В. *Тайна личной корреспонденции в уголовном праве:* Диссертация на соискание ученой степени кандидата юридических наук. Специальность 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Ставрополь, 2003. 160 с.
3. ГОВЕНКО, Ю.А. *Уголовно-правовая охрана тайны частного характера:* Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность 12.00.08 – Уголовное право и криминология; уголовно-исполнительное право. Краснодар: Пятигорский государственный технологический университет, 2010. 26 с.
4. DOBRINOIU, M. Accesul la posta electronică a unei persoane. Posibile încadrări juridice în Romania. În: *Revista de Drept Penal* nr.3, Anul XV, Iulie-Septembrie .https://www.legi-internet.ro/articole-drept-it/accesul-la-poota-electronic-a-unei-persoane-posibile-ncadrri-juridice-n-romnia.html
5. ЦАТУРЯН, Л.А. *Гражданско-правовое регулирование информации:* Автореферат диссертации на соискание ученой степени кандидата юридических наук. Специальность: 12.00.03 – Частное право (гражданское право, торговое (коммерческое) право, международное частное право, семейное право, трудовое право, право социального обеспечения). Ереван: Российско-армянский славянский университет, 2014. 30 с.
6. ЕРШОВ, М.А. *Ответственность за посягательства на конфиденциальную информацию по российскому уголовному праву (проблемы правоприменения и совершенствования законодательства):* Диссертация на соискание ученой степени кандидата юридических наук. Нижний Новгород: Нижегородская академия МВД, 2010. 237 с.
7. Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidentialității și comuni-

caţiilor electronice). În: *Jurnalul Oficial al Uniunii Europene*, L 201, 31.07.2002, p.37-47, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=RO
8. COPEȚCHI, St. Corespondența electronică: obiect imaterial al infracțiunii prevăzute la art.178 CP RM. În: *Studia Universitatis Moldaviae*, 2017, nr.8(108). Seria „*Ştiinţe sociale*", p.116-122. (ISSN 1814-3199, ISSN online 2345-1017)
9. STATI, V. Observaţii critice referitoare la modificările şi completările operate la 22.12.2014 în Hotărârea Plenului Curţii Supreme de Justiţie „Cu privire la practica judiciară în procesele penale despre sustragerea bunurilor", nr.23 din 28.06.2004. În: *Revista Naţională de Drept*, 2015, nr.2, p.2-18. (ISSN 1811-0770)
10. Hotărârea Plenului Curţii Supreme de Justiţie a Republicii Moldova cu privire la practica judiciară în procesele penale despre sustragerea bunurilor, nr.23 din 28.06.2004. În: *Buletinul Curţii Supreme de Justiţie a Republicii Moldova*, 2004, nr.8.
11. Arhiva Curții Supreme de Justiție a Republicii Moldova. Dosarul 1ra-433/2015. Decizia Colegiului penal lărgit din 19 mai 2015.
12. Arhiva Curții Supreme de Justiție a Republicii Moldova. Dosarul nr.1ra-3/2014. Decizia Colegiului penal lărgit din 21 ianuarie 2014.
13. ДИВАЕВА, И.Р. *Некоторые вопросы уголовной ответственности за нарушение неприкосновенности частной жизни*. В: Вестник Челябинского государственного университета, 2009, № 36 (174), Право, Вып.22, с.88. (ISSN 2409-4102)
14. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). În: *Jurnalul Oficial al Uniunii Europene* L 119/1, 04.05.2016.
15. Калмыков Д.А. *Информационная безопасность: понятие, место в системе уголовного законодательства РФ: проблемы правовой охраны:* Диссертация на соискание ученой степени кандидата юридических наук. Специальность 12.00.08 – Уголовное право и криминология; уголовно–исполнительное право. Ярославль: Ярославский государственный университет им. П.Г. Демидова, 2005. 223 с.
16. Legea Republicii Moldova cu privire la schimbul de date și interoperabiltate, nr.142 din 19.07.2018. În: *Monitorul oficial al Republicii Moldova*, 2018, nr.295-308.
17. Legea Republicii Moldova cu privire la protecția datelor cu caracter personal, nr.17-XVI din 15.02.2007. În: *Monitorul Oficial al Republicii Moldova*, 2007, nr.107-111/468.

Date despre autori:
Costică MOȚOC, doctorand, Școala doctorală *Științe Juridice*, Universitatea de Stat din Moldova.
E-mail: ionjan082@gmail.com
ORCID: 0000-0002-1964-2201
Lilia GÎRLA, doctor în drept, conferențiar universitar, Facultatea de Drept, Universitatea de Stat din Moldova.
E-mail: liliagyrla@gmail.com
ORCID: 0000-0002-4979-3027

Prezentat la 16.03.2020