ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXVI/I, ŞTIINȚE JURIDICE, 2020

Protecţia informaţiilor de afaceri: informaţii clasificate, confidenţiale, date cu caracter personal

Protection of business information: classified, confidential, personal data

Ştefan Răzvan Tataru[1]

Rezumat: Afacerile se află într-un proces continuu şi dinamic de adaptare pentru a satisface cererea pieţei şi de a rezista într-un mediu concurenţial. În contextul digitalizării şi internaţionalizării operaţiunilor comerciale şi de cercetare, organizaţiile urmăresc protejarea informaţiilor de afaceri considerate valoroase şi, totodată, conformarea la cerinţele impuse de reglementările din domeniul protecţiei datelor cu caracter personal şi al informaţiilor clasificate. Prezentul studiu evidenţiază tipurile de informaţii utilizate în desfăşurarea afacerilor şi modalităţile de protecţie disponibile. Studiul cuprinde analiza informaţiilor confidenţiale, a celor clasificate, a datelor cu caracter personal şi a informaţiilor publice prelucrate prin activităţi de competitive intelligence.

Cuvinte-cheie: informaţii de afaceri; informaţii confidenţiale; informaţii clasificate; date cu caracter personal; competitive intelligence.

Abstract: Business is in a continuous and dynamic process of adaptation in order to meet the market demand and to withstand in a competitive environment. In the context of the digitization and internationalization of commercial and research operations, organizations seek to protect business information considered valuable, and at the same time to comply with the requirements imposed by the regulations in the field of personal data protection and classified information. The present study highlights the types of information used in business activities and the available means of protection. The study focuses on the analysis of confidential information, classified information, personal data and public information processed through competitive intelligence activities.

Keywords: business information; confidential information; classified information; personal data; competitive intelligence.

Introducere

Protecţia informaţiilor de afaceri şi a datelor cu caracter personal a devenit în prezent un "*must have*" al oricărui profesionist, transformându-se dintr-o preocupare organizaţională considerată de către terţi drept o bună practică, într-un

[1] Doctorand, Facultatea de Drept, Universitatea „Alexandru Ioan Cuza” din Iaşi, email: razvantataru@gmail.com.

standard care oferă siguranţă partenerilor de afaceri şi permite desfăşurarea operaţiunilor comerciale sau de cercetare.

Afacerile desfăşurate pe plan local, naţional sau internaţional se află într-un proces continuu şi dinamic de adaptare pentru a satisface cererea pieţei şi de a rezista într-un mediu concurenţial. În acest context, fiecare organizaţie acordă o mare importanţă acelor elemente care le diferenţiază pe piaţă sau le oferă un avantaj comercial, precum tehnicile de marketing, strategiile de vânzare, clienţii şi furnizorii strategici, reţete sau procese de fabricaţie. Mare parte dintre aceste elemente cheie se prezintă sub formă de informaţii care datorită valorii pe care o prezintă pentru afacere sunt protejate prin desemnarea acestora ca secrete comerciale/informaţii confidenţiale şi asigurarea unor măsuri tehnice şi organizatorice de securizare.

În mod categoric, toate organizaţiile gestionează informaţii confidenţiale, fie că este vorba de propriile lor secrete comerciale, fie în situaţia în care sunt destinatarii unor informaţii confidenţiale primite de la partenerii de afaceri şi asupra cărora au obligaţia de a păstra confidenţialitatea. Totodată, în contextul în care datele cu caracter personal se bucură de o protecţie juridică mai amplă ca niciodată, desfăşurarea operaţiunilor economice la nivel naţional sau internaţional impune asigurarea de măsuri specifice pentru protejarea acestor date. Societăţile comerciale şi alte organizaţii prelucrează datele cu caracter personal ale angajaţilor, reprezentanţilor partenerilor de afaceri şi chiar informaţii privind persoane fizice terţe, fapt care atrage aplicarea legislaţiei din domeniul datelor cu caracter personal. Nu în ultimul rând, desfăşurarea activităţilor comerciale şi de cercetare implică adaptabilitate în modul de lucru cu anumiţi parteneri de afaceri, în special când aceştia sunt instituţii publice sau militare. În aceste situaţii există posibilitatea ca organizaţiile, în procesul de desfăşurare a cooperării, să schimbe atât informaţii confidenţiale, cât şi informaţii clasificate, cele din urmă privind aspecte de interes pentru securitatea naţională sau de interes strategic pentru operatorul economic.

Informaţiile publice nu sunt protejate prin măsuri de securizare şi nici nu mai pot dobândi o valoare comercială, întrucât nu mai pot deveni secrete odată ce au ajuns la cunoştinţa publicului. Aşadar, informaţiile confidenţiale sau secretele comerciale odată ce au fost divulgate publicului acestea nu mai reprezintă o valoare/un activ pentru titular, procesul fiind astfel ireversibil. Cu toate acestea, informaţiile publice pot fi colectate, corelate şi procesate prin intermediul unor procese specifice de *competitive intelligence* rezultând seturi de date valoroase în desfăşurarea afacerilor.

În desfăşurarea afacerilor la nivel naţional sau internaţional, obţinerea şi valorificarea corectă a informaţiilor, inclusiv a celor publice, poate face diferenţa între succesul sau insuccesul unei operaţiuni comerciale.

Tipuri de informaţii utilizate în afaceri

Este de menţionat faptul că atât informaţiile confidenţiale sau clasificate, dar şi datele cu caracter personal pot fi stocate şi gestionate în format fizic sau în

format electronic. Considerăm că informaţiile stocate în format electronic prezintă mult mai multe riscuri decât cele în format fizic întrucât pot fi transferate cu uşurinţă de pe un dispozitiv pe altul, iar prin intermediul resurselor societăţii informaţionale pot fi divulgate publicului sau transmise instant la nivel internaţional.

În cele ce urmează vom analiza modul în care organizaţiile gestionează informaţiile confidenţiale, informaţiile clasificate, datele cu caracter personal şi tehnicile de *competitive intelligence* pentru prelucrarea datelor publice.

1. Informaţiile confidenţiale

Informaţiile confidenţiale reprezintă una din cele mai utilizate şi mai valoroase forme de proprietate intelectuală însă, de cele mai multe ori sunt subevaluate şi neprotejate de către proprietarii lor. Spre deosebire de alte forme de proprietate intelectuală, informaţiile confidenţiale nu implică proceduri sau costuri de înregistrare şi se pot bucura de protecţie un termen nedeterminat, atât timp cât sunt menţinute secret[2].

Confidenţialitatea este acel atribut de securitate prin care se blochează accesul utilizatorilor neautorizaţi la anumite informaţii, fiind o interdicţie şi totodată o excepţie de la utilizarea normală a informaţiei. Protejarea intereselor părţilor implică apărarea secretului comercial şi implicit acceptarea confidenţialităţii[3].

Conform prevederilor Standardului internaţional privind securitatea informaţiei – *ISO/IEC 27000:2018*, confidenţialitatea reprezintă „proprietatea conform căreia informaţiile nu sunt puse la dispoziţie sau dezvăluite unor persoane, entităţi sau procese neautorizate”[4].

Informaţiile confidenţiale nu beneficiază de o definiţie legală, reglementările actuale făcând trimitere la concepte precum informaţiilor de afaceri nedivulgate, know-how[5], secrete comerciale[6], secrete de afaceri[7] sau informaţii

---

[2] Pentru similitudine, a se vedea: C.T. Ungureanu, *op. cit.*, pp. 118-119; CHINA IPR SME HelpDesk, *op. cit.*, pp. 1-2.

[3] B.D. Ţigănoaia, *Asigurarea securităţii informaţiilor în organizaţii*, Editura Institutul European, Iaşi, 2013, p. 34.

[4] A se vedea Standardul *ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary*, elaborat de Organizaţia Internaţională pentru Standardizare (International Organization for Standardization), [Online] adresa: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.

[5] *Know how*-ul reprezintă un ansamblu de cunoştinţe tehnice nebrevetate şi transmisibile, necesare în fabricarea unui produs sau elaborarea unui procedeu. A se vedea I. Macovei, *Tratat de drept al comerţului internaţional*, Editura Universul Juridic, Bucureşti, 2014, p. 426; C.T. Ungureanu, *Dreptul comerţului internaţional. Contracte de comerţ internaţional*, Editura Hamangiu, 2014, p. 118.

[6] A se vedea O.U.G. nr. 25/2019 privind protecţia know-how-ului şi a informaţiilor de afaceri nedivulgate care constituie secrete comerciale împotriva dobândirii, utilizării şi

care nu sunt destinate publicităţii[8], secrete de fabricaţie[9], secrete industriale sau profesionale[10]. Apreciem că toate conceptele menţionate sunt incluse în conceptul mai larg de „informaţii confidenţiale".

Considerăm că „informaţiile confidenţiale" desemnează acele informaţii fără caracter public, privind organizaţia, activităţile sale sau operaţiunile în care este implicată, care au valoare comercială şi fac obiectul unor măsuri de protecţie împotriva accesului neautorizat sau a divulgării publice[11].

La nivel internaţional, informaţiile confidenţiale de afaceri sunt definite în cadrul Acordului TRIPS (*The Agreement on Trade-Related Aspects of Intellectual Property Rights*) drept acele informaţii cu caracter secret şi valoare comercială, asupra cărora deţinătorul legitim a luat măsuri rezonabile pentru a le asigura confidenţialitatea[12].

O definiţie a conceptului de informaţie confidenţială întâlnim în conţinutul Modelului de contract de confidenţialitate elaborat de Camera Internaţională de Comerţ de la Paris[13], acesta reprezentând „*orice informaţie [...] comunicată de către sau în numele părţii divulgatoare către partea destinatară, incluzând, dar fără a se limita la, orice fel de informaţii de afaceri, informaţii comerciale sau tehnice [...], cu excepţia informaţiilor care, în mod evident, nu au caracter confidenţial*".

Sfera informaţiilor confidenţiale este determinată de fiecare organizaţie în parte, acestea stabilind exact categoriile de informaţii de afaceri considerate confidenţiale şi măsurile de protecţie ale acestora. Societăţile pot aprecia ca fiind

---

divulgării ilegale, precum şi pentru modificarea şi completarea unor acte normative, publicată în M. Of. nr. 309 din 19 aprilie 2019.

7 A se vedea art. 45 din Legea concurenţei nr. 21/1996, varianta consolidată, republicată în M. Of. nr. 153 din 29 februarie 2016.

8 A se vedea art. 304 din Legea nr. 286 din 17 iulie 2009 privind Codul penal, publicată în M. Of. nr. 510 din 24 iulie 2009.

9 A se vedea art. 58 din Legea nr. 64/1991 privind brevetele de invenţie, republicată în M. Of. nr. 613 din 19 august 2014.

10 A se vedea art. 283^3 din Codul de procedură fiscală din 2015, publicat în M. Of. nr. 547 din 23 iulie 2015.

11 Pentru similitudine a se vedea D. Castraveţ, *Unele consideraţii privind divulgarea secretului comercial*, în volumul Conferinţei „Integrare prin cercetare şi inovare" – Ştiinţe juridice. vol. 2, 28-29 septembrie 2016, Chişinău, 2016, pp. 11-14, articol [Online] adresa: https://ibn.idsi.md/vizualizare_articol/75947; China IPR SME HelpDesk, *Protecting Your Trade Secrets in China*, p. 2, material [Online] adresa: https://www.china-iprhelpdesk.eu/sites/all/docs/publications/EN_Trade_Secrets_Nov_2010.pdf.

12 A se vedea art. 39 alin. (2) din Acordul TRIPS, disponibil la adresa: https://www.wto.org/english/docs_e/legal_e/31bis_trips_04d_e.htm#7. Pentru similitudine a se vedea: O.M. Florescu, *Acordul TRIPS, acord multilateral al OMC* în Theoretical and Applied Economics, No. 6/2006, p. 67, articol [Online] adresa: http://store.ectap.ro/articole/112.pdf; D. Castraveţ, *op. cit.*, p. 11.

13 A se vedea International Chamber of Commerce, ICC Model Confidentiality Agreement, Editura ICC SERVICES Publications Department, Paris, 2006, [Online] adresa: https://epdf.pub/icc-model-confidentiality-agreement.html.

confidenţiale o categorie vastă de informaţii, incluzând procese de fabricare, invenţii aflate în faze incipiente, planuri şi strategii de marketing sau de vânzare, metodele de prospectare a pieţei, de distribuţie, bazele de date cu furnizori şi/sau clienţi, planuri de investiţii, proiecte de cercetare-dezvoltare[14].

1.1. Reglementare

La nivelul Uniunii Europene, informaţiile confidenţiale sau secretele comerciale au fost reglementate prin Directiva (UE) 2016/943 privind protecţia know-how-ului şi a informaţiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării şi divulgării ilegale. Conform art. 2 pct. 1 din Directivă, informaţiile confidenţiale sau secretele comerciale reprezintă acele informaţii care au o valoare comercială prin faptul că sunt secrete, fac obiectul unor măsuri rezonabile de securizare şi protecţie, şi a căror divulgare neautorizată ar putea genera un prejudiciu economic, de imagine sau dezavantaj competitiv societăţii deţinătoare a secretelor comerciale[15].

În România, secretele comerciale sunt definite în cadrul art. 1^1 lit. d) din Legea nr. 11/1991[16] drept „informaţiile care îndeplinesc cumulativ următoarele cerinţe: 1. sunt secrete în sensul că nu sunt, ca întreg sau astfel cum se prezintă sau se articulează elementele acestora, cunoscute la nivel general sau uşor accesibile persoanelor din cercurile care se ocupă, în mod normal, de tipul de informaţii în cauză; 2. au valoare comercială prin faptul că sunt secrete; 3. au făcut obiectul unor măsuri rezonabile, în circumstanţele date, luate de către persoana care deţine în mod legal controlul asupra informaţiilor respective, pentru a fi păstrate secrete".

În categoria informaţiilor confidenţiale includem şi „informaţiile privilegiate" utilizate pe piaţa de capital. Conform Legii nr. 24/2017 privind emitenţii de instrumente financiare şi operaţiuni de piaţă[17], prin „informaţie privilegiată" se înţelege „o informaţie cu caracter precis care nu a fost făcută publică, care se referă în mod direct sau indirect la unul sau mai mulţi emitenţi ori la unul sau mai multe instrumente financiare, şi care, dacă ar fi făcută publică, ar putea

[14] Pentru similitudine, a se vedea C.T. Ungureanu, *op. cit.*, p. 119; M. Boancă-Ivan, *Clauzele specifice în contractele de comerţ internaţional*, Teză de doctorat, Universitatea Alexandru Ioan Cuza din Iaşi, Facultatea de Drept, Iaşi, 2015, p. 69.

[15] Conform art. 2 din Directiva (UE) nr. 2016/943 a Parlamentului European şi a Consiliului din 8 iunie 2016 privind protecţia know-how-ului şi a informaţiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării şi divulgării ilegale, în J.O. UE nr. L 157 din data de 16 iunie 2016 şi transpusă în legislaţia naţională prin Ordonanţa de urgenţă nr. 25/2019 privind protecţia know-how-ului şi a informaţiilor de afaceri nedivulgate care constituie secrete comerciale împotriva dobândirii, utilizării şi divulgării ilegale, precum şi pentru modificarea şi completarea unor acte normative, publicată în M. Of. nr. 309 din 19 aprilie 2019.

[16] Legea nr. 11/1991 privind combaterea concurenţei neloiale, publicată în M. Of. nr. 24 din 30 ianuarie 1991.

[17] Legea nr. 24/2017 privind emitenţii de instrumente financiare şi operaţiuni de piaţă, publicată în M. Of. nr. 213 din 29 martie 2017.

influenţa semnificativ preţul acelor instrumente financiare sau preţul instrumentelor financiare derivate conexe". Informaţia cu caracter precis reprezintă „acea informaţie care indică un set de circumstanţe care există sau despre care se poate estima în mod rezonabil că vor exista, sau un eveniment care s-a produs sau se poate estima în mod rezonabil că se va produce şi pe baza căreia, datorită naturii specifice a acesteia, se poate trage o concluzie cu privire la efectul pe care îl pot avea respectivele circumstanţe sau respectivul eveniment asupra preţului instrumentelor financiare, asupra preţului instrumentelor financiare derivate conexe, asupra preţului contractelor spot pe mărfuri conexe sau asupra preţului produselor licitate pe baza certificatelor de emisii"[18].

Informaţiile confidenţiale pot prezenta o importanţă atât de mare, încât o dată divulgate, organizaţia care le deţinea să fie eliminată de pe piaţă. Organizaţia a cărei informaţii au fost divulgate, în mod intenţionat sau din neglijenţă, poate suferi un prejudiciu economic capabil să determine intrarea în insolvenţă sau poate genera un dezavantaj competitiv iremediabil, ca urmare fie a valorificării respectivelor informaţii de către societăţile concurente, fie a unei sancţiuni dispuse de autorităţile din domeniul concurenţei pentru influenţarea preţurilor sau comportamentelor pe piaţă[19].

1.2. Modalităţi de protecţie

Informaţiile confidenţiale pot fi protejate prin instituirea unor bariere fizice, tehnice şi contractuale menite să limiteze accesul la informaţii, să asigure o trasabilitate a modului în care au fost accesate şi utilizate datele respective şi să poată asigura identificarea incidentelor la securitatea datelor şi autorul acestora[20].

Barierele fizice pot presupune implementarea unor măsuri care să vizeze accesul la datele în format fizic, precum: marcarea documentelor cu menţiunea „Confidenţial", stocarea documentelor confidenţiale în locaţii securizate cu încuietori, stabilirea unor nivele de acces pentru salariaţi, limitarea posibilităţilor de copiere şi transmitere a informaţiilor confidenţiale.

Barierele tehnice constau în asigurarea securităţii resurselor informatice şi a informaţiilor confidenţiale în format electronic. În această situaţie, principalele măsuri ce pot fi luate de către societăţi constau în implementarea de măsuri de securitate informatică, precum utilizarea de programe software doar cu licenţă, instalarea unor programe antivirus, dar şi în elaborarea unor politici interne de utilizare a resurselor informatice şi instruirea angajaţilor în acest domeniu. Poate unul dintre cele mai utile instrumente de securizare a informaţiilor confidenţiale în format electronic este reprezentat de utilizarea unui program dedicat prevenţiei scurgerii de date (*Data Loss Prevention)* – soluţie software care iden-

[18] Conform art. 114 alin. (5) din Legea nr. 24/2017 privind emitenţii de instrumente financiare şi operaţiuni de piaţă.

[19] Ş.R. Tataru, *Soluționarea litigiilor referitoare la contractele de comerț internațional cu produse farmaceutice*, Teză de doctorat, Universitatea Alexandru Ioan Cuza din Iaşi, Facultatea de Drept, Iaşi, 2020, p. 39; D. Castraveţ, *op. cit.,* p. 11.

[20] A se vedea China IPR SME HelpDesk, *op. cit.*, p. 1.

tifică şi monitorizează modul în care datele confidenţiale sunt stocate sau utilizate de către utilizator pe calculator, email, *cloud* şi alte sistemele de stocare[21].

Barierele contractuale constau în utilizarea acordurilor de confidenţialitate în interiorul organizaţiei şi în exteriorul acesteia. Astfel, este recomandat ca organizaţia deţinătoare de informaţii confidenţiale să încheie acorduri de confidenţialitate cu salariaţii care au acces la date confidenţiale. În situaţia în care societatea intră în afaceri care implică transferul de informaţii confidenţiale este recomandat să încheie contracte de confidenţialitate (*Confidential Agreement* sau *Non-Disclosure Agreement*) cu respectivele organizaţii partenere. În cazul ambelor tipuri de acorduri de confidenţialitate, deţinătorul informaţiilor trebuie să manifeste diligenţă în definirea datelor confidenţiale care vor fi transmise[22] şi să se asigure că partenerul contractual va respecta obligaţia de confidenţialitate.

1.3. Sancţionarea încălcării obligaţiei de confidenţialitate

Dobândirea, utilizarea şi divulgarea ilegală a informaţiilor confidenţiale poate atrage, după caz, răspunderea civilă contractuală, răspunderea civilă delictuală, răspunderea contravenţională sau răspunderea penală a autorului[23].

Conform art. 4 din O.U.G. nr. 25/2019, deţinătorii de informaţii confidenţiale pot solicita instanţei de judecată competente aplicarea măsurilor, procedurilor şi acţiunilor reparatorii prevăzute de lege pentru a preveni sau împiedica dobândirea, utilizarea sau divulgarea ilegală a secretelor lor comerciale sau pentru a obţine reparaţii în urma unor astfel de fapte.

La cererea părţii prejudiciate, instanţa poate dispune obligarea autorului încălcării, care ştia sau ar fi trebuit să ştie că se implică în dobândirea, utilizarea sau divulgarea ilegală a unui secret comercial, la plata de daune-interese proporţionale cu prejudiciul real suferit ca urmare a dobândirii, utilizării sau divulgării ilegale a secretului comercial[24].

În ipoteza încălcării obligaţiilor asumate printr-un acord de confidenţialitate sau printr-o clauză contractuală de confidenţialitate, proprietarul informaţiilor confidenţiale poate solicita instanţei angajarea răspunderii civile contractuale a părţii debitoare a obligaţiei de confidenţialitate şi obligarea acesteia la plata de daune interese[25].

De asemenea, proprietarul informaţiilor confidenţiale poate solicita angajarea răspunderii civile delictuale a terţului care, având cunoştiinţă de caracterul confidenţial al informaţiilor, le-a divulgat sau le-a exploatat fără drept[26].

---

21 A se vedea https://www.romsym.ro/product.php/Symantec-Data-Loss-Prevention/693/ (17.04.2020) şi https://www.proofpoint.com/us/glossary/dlp (17.04.2020).

22 C.T. Ungureanu, *op. cit.*, p. 119; D.A. Sitaru, *op. cit.*, p. 444.

23 Pentru similitudine, a se vedea M. Boancă Ivan, *op. cit.*, p. 74.

24 Conform art. 14 alin. (1) din O.U.G. nr. 25/2019.

25 Pentru similitudine, a se vedea: C.T. Ungureanu, *op. cit.*, p. 119; D.A. Sitaru, *Dreptul comerţului internaţional. Partea generală*, ed. a II-a, revizuită şi adăugită, Editura Universul Juridic, Bucureşti, 2017, pp. 444-445; M. Boancă Ivan, *op. cit.*, p. 74.

26 Pentru similitudine, a se vedea M. Boancă Ivan, *op. cit.*, p. 74.

Totodată, divulgarea informaţiilor confidenţiale poate atrage răspunderea penală a autorului faptei în temeiul art. 304 – *Divulgarea informaţiilor secrete de serviciu sau nepublice*[27] şi art. 308 – *Infracţiuni de corupţie şi de serviciu comise de alte persoane*[28] din Codul penal român care prevăd pedeapsa cu închisoarea sau cu amendă pentru divulgarea, fără drept, a unor informaţii care nu sunt destinate publicităţii, de către cel care le cunoaşte datorită atribuţiilor de serviciu sau ia cunoştinţă de acestea, dacă prin aceasta sunt afectate interesele sau activitatea unei persoane.

Răspunderea contravenţională sau penală a persoanei care divulgă sau utilizează fără drept un secret comercial poate fi atrasă şi în temeiul prevederilor Legii nr. 11/1991[29] privind combaterea concurenţei neloiale, art. 4 alin. (1) şi (2)[30], respectiv art. 5 lit. c)[31].

2. Informaţiile clasificate

Informaţiile clasificate sunt, de cele mai multe ori, utilizate în cadrul autorităţilor publice întrucât acestea privesc date a căror divulgare poate prejudicia

---

27 Extras din Codul Penal: „*Art. 304. (1) Divulgarea, fără drept, a unor informaţii secrete de serviciu sau care nu sunt destinate publicităţii, de către cel care le cunoaşte datorită atribuţiilor de serviciu, dacă prin aceasta sunt afectate interesele sau activitatea unei persoane, se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă. (2) Divulgarea, fără drept, a unor informaţii secrete de serviciu sau care nu sunt destinate publicităţii, de către cel care ia cunoştinţă de acestea, se pedepseşte cu închisoare de la o lună la un an sau cu amendă*".

28 Extras din Codul Penal: „*Art. 308. (1) Dispoziţiile [...] art. 304 privitoare la funcţionarii publici se aplică în mod corespunzător şi faptelor săvârşite de către sau în legătură cu persoanele care exercită, permanent ori temporar, cu sau fără o remuneraţie, o însărcinare de orice natură în serviciul unei persoane fizice prevăzute la art. 175 alin. (2) ori în cadrul oricărei persoane juridice. (2) În acest caz, limitele speciale ale pedepsei se reduc cu o treime*".

29 Legea nr. 11/1991 privind combaterea concurenţei neloiale, publicată în M. Of. nr. 24 din 30 ianuarie 1991.

30 Extras din Legea nr. 11/1991: Art. 2 alin. (2): „*Sunt interzise practicile de concurenţă neloială, după cum urmează: b) deturnarea clientelei unei întreprinderi de către un fost sau actual salariat/reprezentant al său ori de către orice altă persoană prin folosirea unor secrete comerciale, pentru care respectiva întreprindere a luat măsuri rezonabile de asigurare a protecţiei acestora şi a căror dezvăluire poate dăuna intereselor acelei întreprinderi*". Art. 4: „*(1) Constituie contravenţii, în măsura în care nu sunt săvârşite în astfel de condiţii încât să fie considerate potrivit legii penale infracţiuni, încălcarea cu vinovăţie a prevederilor art. 2 alin. (2) lit. a) şi b). (2) Contravenţiile prevăzute la alin. (1) se sancţionează cu: a) amendă de la 5.000 lei la 50.000 lei pentru contravenţiile săvârşite de persoane juridice; b) amendă de la 5.000 lei la 10.000 lei pentru contravenţiile săvârşite de persoane fizice".*

31 Extras din Legea nr. 11/1991: Art. 5 „*Constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă: c) divulgarea, achiziţionarea sau utilizarea secretului comercial de către terţi, ca rezultat al unei acţiuni de spionaj comercial ori industrial, dacă prin aceasta sunt afectate interesele sau activitatea unei persoane juridice*".

siguranţa naţională şi apărarea ţării sau interesele unei persoane juridice de drept public sau privat. Organizaţiile de drept privat, precum societăţile comerciale sau institutele de cercetare ştiinţifică, pot utiliza informaţii clasificate în trei situaţii: 1. ca urmare a desemnării unor informaţii proprii drept secrete de serviciu, conform Legii nr. 182/2002 privind informaţiile clasificate şi Hotărârii de Guvern nr. 781/2002 privind protecţia informaţiilor secrete de serviciu; 2. în vederea participării la procedura de negociere a unui contract clasificat şi pe perioada desfăşurării acestuia (de exemplu, o societate comercială producătoare de tehnică militară sau de echipamente medicale este interesată să participe în cadrul unei licitaţii organizate de Ministerul Apărării Naţionale); şi 3. în vederea derulării unor activităţi industriale şi/sau de cercetare ce presupun accesul la informaţii clasificate (de exemplu, în cazul unui parteneriat cu o autoritate/instituţie publică în vederea cercetării-dezvoltării unui produs).

2.1. Concept şi reglementare

În România, informaţiile clasificate sunt reglementate prin Legea nr. 182/2002 privind protecţia informaţiilor clasificate[32], Hotărârea nr. 585/2002 pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România[33] şi Hotărârea nr. 781/2002 privind protecţia informaţiilor secrete de serviciu[34].

Conform art. 15 lit. b) din Legea nr. 182/2002, informaţiile clasificate reprezintă „*informaţiile, datele, documentele de interes pentru securitatea naţională, care, datorită nivelurilor de importanţă şi consecinţelor care s-ar produce ca urmare a dezvăluirii sau diseminării neautorizate, trebuie să fie protejate*".

2.2. Categorii de informaţii clasificate

Conform Legii nr. 182/2002, informaţiile clasificate pot fi categorisite, în funcţie de clasele de secretizare, în secrete de stat şi secrete de serviciu. Informaţiile secrete de stat sunt acele „*informaţii care privesc securitatea naţională, prin a căror divulgare se pot prejudicia siguranţa naţională şi apărarea ţării*", iar informaţiile secrete de serviciu, acele „*informaţii a căror divulgare este de natură să determine prejudicii unei persoane juridice de drept public sau privat*".

2.2.1. Informaţiile secret de stat

La nivel naţional, conform art. 15 lit. f) din Legea nr. 182/2002, informaţiile secret de stat pot fi diferenţiate, în funcţie de nivelul de secretizare atribuit, astfel:

[32] Legea nr. 182/2002 privind protecţia informaţiilor clasificate, publicată în M. Of. nr. 248 din 12 aprilie 2002.

[33] Hotărârea nr. 585/2002 pentru aprobarea Standardelor naţionale de protecţie a informaţiilor clasificate în România, publicată în M. Of. nr. 485 din 5 iulie 2002.

[34] Hotărârea nr. 781/2002 privind protecţia informaţiilor secrete de serviciu, publicată în M. Of. nr. 575 din 5 august 2002.

- informaţii secret de stat, nivel strict secret de importanţă deosebită – informaţiile a căror divulgare neautorizată este de natură să producă daune de o gravitate excepţională securităţii naţionale;

- informaţii secret de stat, nivel strict secret – informaţiile a căror divulgare neautorizată este de natură să producă daune grave securităţii naţionale;

- informaţii secret de stat, nivel secret – informaţiile a căror divulgare neautorizată este de natură să producă daune securităţii naţionale.

2.2.2. Informaţiile secret de serviciu

Legislaţia românească privind protecţia informaţiilor clasificate permite societăţilor comerciale să îşi protejeze informaţiile considerate foarte valoroase afacerii prin desemnarea acestora ca informaţii clasificate – secrete de serviciu. Comparativ cu informaţiile confidenţiale, desemnarea de către o societate a unor informaţii ca secrete de serviciu conferă un grad mai mare de protecţie prin măsurile obligatorii ce trebuie implementate şi determină, în mod indirect, responsabilizarea personalului care are acces şi gestionează respectivele date.

Conform art. 32 din Legea nr. 182/2002, „*conducătorii autorităţilor şi instituţiilor publice, ai agenţilor economici cu capital integral sau parţial de stat şi ai altor persoane juridice de drept public ori privat sunt obligaţi să stabilească informaţiile care constituie secrete de serviciu şi regulile de protecţie a acestora, să coordoneze activitatea şi să controleze măsurile privitoare la păstrarea secretului de serviciu, potrivit competenţelor*". Observăm că spre deosebire de informaţiile secret de stat, informaţiile secret de serviciu se stabilesc de conducătorul persoanei juridice[35].

Totodată, legislaţia în vigoare interzice clasificarea ca secrete de serviciu a informaţiilor care, prin natura sau conţinutul lor, sunt destinate să asigure informarea cetăţenilor asupra unor probleme de interes public sau personal, pentru favorizarea ori acoperirea eludării legii sau obstrucţionarea justiţiei[36].

2.2.3. Informaţii clasificate la nivel regional şi internaţional

La nivelul Uniunii Europene, informaţiile clasificate reprezintă „*orice informaţii sau materiale desemnate ca atare printr-o clasificare de securitate a UE a căror divulgare neautorizată ar cauza prejudicii de diferite grade intereselor Uniunii Europene sau ale unora sau mai multor state membre*". Acestea sunt clasificate pe patru niveluri în a) EU Top Secret; b) EU Secret; c) EU Confidential; d) EU Restricted[37].

La nivelul statelor membre ale Organizaţiei Tratatului Atlanticului de Nord (NATO), informaţiile clasificate NATO „se referă la toate informaţiile clasificate de natură politică, militară şi economică, vehiculate în cadrul NATO, elaborate în cadrul structurilor NATO sau primite de la statele membre ori de la alte

[35] Conform art. 31 din Legea nr. 182/2002 privind protecţia informaţiilor clasificate.

[36] Conform art. 33 din Legea nr. 182/2002 privind protecţia informaţiilor clasificate.

[37] Conform art. 2 din Decizia Consiliului nr. 2013/488/UE privind normele de securitate pentru protecţia informaţiilor UE clasificate, în J.O. UE nr. L 274/1 din 15 octombrie 2013.

organizaţii internaţionale”[38]. În cadrul NATO informaţiile sunt clasificate pe patru niveluri şi anume: Cosmic Top Secret, NATO Secret, NATO Confidential şi NATO Restricted[39].

2.3. Modalităţi de protecţie

În situaţia în care o organizaţie de drept privat intră în relaţii contractuale care impun utilizarea de informaţii clasificate, aceasta va trebui să se asigure că implementează cu stricteţe măsurile de securizare şi protecţie a informaţiilor respective, conform reglementărilor speciale incidente. Spre deosebire de informaţiile confidenţiale, situaţie în care organizaţia ar putea implementa în mod discreţionar măsurile de protecţie pe care le-ar considera oportune, în cazul informaţiilor clasificate, implementarea măsurilor este obligatorie şi reprezintă condiţie prealabilă pentru a obţine avizele[40], autorizaţiile[41] şi certificările[42] necesare utilizării acestei categorii de date[43].

2.4. Răspunderea în domeniul informaţiilor clasificate

Legea nr. 182/2002 stabileşte în cadrul art. 37 alin. (2) faptul că răspunderea privind protecţia informaţiilor clasificate revine conducătorului autorităţii sau instituţiei publice ori altei persoane juridice deţinătoare de informaţii, după caz. Încălcarea normelor privind protecţia informaţiilor clasificate poate atrage răspunderea disciplinară, contravenţională, civilă sau penală, în condiţiile prevăzute de Legea nr. 182/2002 şi H.G. nr. 585/2002.

---

38 Conform cap. B pct. 10 din Norma privind protecţia informaţiilor clasificate ale Organizaţiei Tratatului Atlanticului de Nord în România din 15.04.2002, publicată în M. Of. nr. 315 din 13 mai 2002.

39 A se vedea website-ul NATO la adresa: https://www.nato.int/cps/en/natohq/declassified_138449.htm.

40 Aviz de securitate industrială – document eliberat de către ADS prin care se atestă că obiectivul industrial contractant a implementat toate măsurile de securitate necesare protecţiei informaţiilor clasificate vehiculate în derularea contractului încheiat – conform art. 3 din Standardele naţionale de protecţie a informaţiilor clasificate în România.

41 Autorizaţie de securitate industrială – document eliberat de Oficiul Registrului Naţional al Informaţiilor Secrete de Stat (ORNISS) unui obiectiv industrial, prin care se atestă că este abilitat să participe la procedura de negociere a unui contract clasificat – conform art. 3 din Standardele naţionale de protecţie a informaţiilor clasificate în România.

42 Certificat de securitate industrială – document eliberat de ORNISS unui obiectiv industrial, prin care se atestă că este abilitat să deruleze activităţi industriale şi/sau de cercetare ce presupun accesul la informaţii clasificate – conform art. 3 din Standardele naţionale de protecţie a informaţiilor clasificate în România.

43 A se vedea prevederile Capitolului VII Securitatea Industrială din cadrul Standardelor naţionale de protecţie a informaţiilor clasificate în România, publicată în M. Of. nr. 485 din 5 iulie 2002.

Răspunderea penală pentru divulgarea informaţiilor clasificate este reglementată în cadrul Codului penal, art. 303 – *Divulgarea informaţiilor secrete de stat*, respectiv art. 304 – *Divulgarea informaţiilor secrete de serviciu sau nepublice*. Astfel, în cazul documentelor clasificate secret de stat, divulgarea, fără drept, a unor informaţii secrete de stat, de către cel care le cunoaşte datorită atribuţiilor de serviciu, dacă prin aceasta sunt afectate interesele unei autorităţi sau instituţii publice, se pedepseşte cu închisoarea de la 2 la 7 ani şi interzicerea exercitării unor drepturi.

Similar divulgării informaţiilor confidenţiale, persoana care divulgă fără drept informaţii secrete de serviciu poate răspunde penal, dacă sunt îndeplinite condiţiile impuse de art. 304 Cod penal.

3. Datele cu caracter personal

În desfăşurarea operaţiunilor comerciale, organizaţiile prelucrează în mod inevitabil date cu caracter personal, fie că obiectul de activitate implică prelucrări de baze de date cu caracter personal, fie că se rezumă la prelucrarea datelor propriilor angajaţi. În ambele situaţii, societatea este obligată să implementeze măsuri tehnice şi organizatorice pentru a asigura conformitatea cu standardele şi cerinţele impuse de legislaţia din domeniul datelor cu caracter personal.

3.1. Concept şi reglementare

Începând cu anul 2016, protecţia datelor cu caracter personal a fost reglementată în mod unitar la nivelul Uniunii Europene prin Regulamentul (UE) nr. 2016/679[44] privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date, denumit şi Regulamentul general privind protecţia datelor (RGPD).

Conform prevederilor art. 4 pct. 1 din Regulamentul General privind Protecţia Datelor, datele cu caracter personal sunt acele informaţii care privesc o persoană fizică identificată ori identificabilă. „O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale". Regulamentul delimitează o categorie specială de date, şi anume datele sensibile care conduc la identificarea garantată a unei anumite persoane datorită caracterului originar, original şi unic: datele privind sănătatea, datele biologice şi datele genetice[45].

---

[44] Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE, publicat în J.O. UE nr. L 119, din data de 4 mai 2016.

[45] S.R. Tataru, A. Şerban, *Protecţia datelor cu caracter personal ale participanţilor la studiile clinice*, în Revista Dreptul nr. 2/2019, p. 21.

Prin prelucrare de date cu caracter personal înţelegem „*orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal [...], cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea*”[46].

Spre deosebire de informaţiile confidenţiale şi cele clasificate, unde protecţia vizează interesele organizaţiei sau autorităţii care le deţine, titularul dreptului la protecţia datelor cu caracter personal este persoana fizică, numită „persoană vizată”[47].

În derularea afacerilor, rolul de persoană vizată poate fi avut de către angajaţi, reprezentanţii societăţilor partenere, clienţii persoane fizice – consumatorii, persoane terţe în cazul în care le sunt prelucrate datele cu caracter personal. În sfera datelor cu caracter personal, prelucrate în desfăşurarea afacerilor, pot fi incluse o varietate de informaţii privind persoana fizică precum:

- Datele angajaţilor organizaţiei: date de identificare (de exemplu: nume, prenume, cod numeric personal, serie şi număr carte de identitate), date de contact (de exemplu: adresa, număr de telefon, adresă de email), date privind nivelul de pregătire şi experienţa profesională (informaţii din Curriculum vitae, atestate, certificări), date privind situaţia economică (nivel salarizare, cuantum bonusuri), date medicale etc.
- Datele reprezentanţilor societăţilor partenere: date de identificare (nume, prenume), date de contact (număr de telefon mobil, adresă de email de serviciu, adresă profesională) etc.
- Datele consumatorilor: în funcţie de serviciul prestat sau bunul comercializat, date de identificare (nume, prenume, identificatori unici), date de contact (adresă de domiciliu, număr de telefon, adresă de email), preferinţele sau comportamentul consumatorului[48] etc.

Apreciem că în desfăşurarea operaţiunilor comerciale sau de cercetare pot fi prelucrate o varietate de date cu caracter personal, volumul şi categoriile de date prelucrate variind în funcţie de obiectul de activitate al societăţii şi scopul stabilit de operator.

Prelucrarea datelor cu caracter personal în conformitate cu principiile şi standardele impuse de RGPD este cu atât mai importantă cu cât societăţile, în desfăşurarea afacerilor, gestionează date sensibile şi a căror prelucrare

---

46 Conform art. 4 pct. 2 din Regulamentul (UE) 2016/679.

47 C.T. Ungureanu, *Protecţia datelor cu caracter personal în contractele internaţionale,* în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi, Tomul LXIII, Ştiinţe Juridice, nr. 2/2017, p. 141.

48 A. Şerban, *The Value of Privacy: What Does the Personal Data Mean to the Data Subject and Businesses?* în K. Strada-Rozenberga, M. do Rosário Anjos (eds.), *Current Issues in Business Law*, Editura Adjuris International Academic Publisher, Bucureşti, 2018, pp. 121-123, [Online], consultat în 15.04.2020: http://www.adjuris.ro/reviste/ciibl/Current%20Issues%20in%20Business%20Law.pdf.

neconformă sau divulgare neautorizată poate genera un risc ridicat pentru drepturile şi libertăţile persoanelor.

La nivel naţional, prin prevederile Legii nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) nr. 2016/679[49], legiuitorul român a stabilit reguli speciale privind prelucrarea unor categorii de date cu caracter personal şi, implicit, obligaţii suplimentare în sarcina organizaţiilor care prelucrează date cu caracter personal.

3.2. Modalităţi de protecţie

Conform Regulamentului RGPD, răspunderea pentru protecţia datelor cu caracter personal revine operatorului şi persoanei împuternicite de către acesta. Operatorul este persoana fizică sau juridică, care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal[50].

Datele cu caracter personal pot fi protejate prin instituirea unor măsuri tehnice şi organizatorice de securizare a datelor în format fizic şi electronic. Poate primordial oricărei măsuri de protecţie este implementarea conceptelor *privacy by design* şi *privacy by default* (art. 25 RGPD – *Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit*), dar şi respectarea principiilor de prelucrare a datelor stabilite de RGPD[51].

Prelucrarea datelor cu caracter personal în conformitate cu prevederile Regulamentului general privind protecţia datelor trebuie realizată cu respectarea următoarelor şapte principii generale[52]:

a) Legalitate, echitate şi transparenţă – datele cu caracter personal trebuie prelucrate într-un mod legal şi transparent, garantând echitatea în ceea ce priveşte persoanele fizice ale căror date cu caracter personal sunt prelucrate;
b) Limitarea scopului – trebuie să existe scopuri specifice ale prelucrării datelor, operatorul fiind obligat să informeze persoanele fizice în legătură cu scopurile respective atunci când le colectează date cu caracter personal;
c) Reducerea datelor – operatorul trebuie să colecteze şi să prelucreze numai acele date cu caracter personal care sunt necesare pentru îndeplinirea scopului;

[49] Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), varianta consolidată, publicată în M. Of. nr. 651 din 26 iulie 2018.

[50] Conform art. 4 pct. 7 din Regulamentul (UE) 2016/679.

[51] Pentru mai multe detalii privind principiile de prelucrare a datelor cu caracter personal, a se vedea A. Iftimiei, *Protecţia datelor cu caracter personal. Aspecte de drept european,* în Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza" din Iaşi, Ştiinţe Juridice, Tomul LXIV, nr. 1/2018, pp. 275-280.

[52] A se vedea Information Commissioner's Office Website, la adresa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/.

d) Exactitatea datelor – operatorul trebuie să se asigure că datele cu caracter personal sunt exacte şi actualizate, având în vedere scopurile pentru care sunt prelucrate;
e) Limitarea stocării – operatorul trebuie să se asigure că datele cu caracter personal nu sunt stocate mai mult timp decât este necesar pentru scopurile în care au fost colectate;
f) Integritate şi confidenţialitate (securitate) – operatorul trebuie să prevadă garanţii tehnice şi organizaţionale adecvate care să asigure securitatea datelor cu caracter personal[53];
g) Responsabilitate – în activităţile de prelucrare a datelor, operatorul trebuie să manifeste responsabilitate şi să poate demonstra conformitatea cu principiile enunţate mai sus.

Printre principalele obligaţii ale operatorilor de date putem enumera: a) identificarea prelucrărilor de date cu caracter personal efectuate şi păstrarea evidenţei activităţilor de prelucrare; b) desemnarea unui responsabil cu protecţia datelor; c) cartografierea fluxurilor de date în organizaţie; d) asigurarea protecţiei datelor prin măsuri tehnice şi organizaţionale; e) în caz de încălcare a securităţii datelor, operatorul trebuie să informeze autoritatea de supraveghere şi persoanele vizate, dacă evenimentul este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile acestora din urmă.

Nerespectarea măsurilor de securitate şi a condiţiilor impuse de legislaţie pentru prelucrarea conformă a datelor cu caracter personal poate determina atingeri asupra drepturilor persoanei fizice şi poate genera inclusiv prejudicii patrimoniale.

3.3. Răspunderea operatorului

În situaţia în care organizaţiile (operatorii) nu respectă obligaţiile impuse de prevederile RGPD, acestea pot fi sancţionate de către autoritatea de supraveghere cu amenzi în cuantum de până la 20 milioane de euro sau de până la 4% din cifra de afaceri la nivel internaţional.

Cumulativ cu sancţiunea dispusă de autoritatea de supraveghere, operatorul care a prelucrat neconform datele cu caracter personal ale persoanei vizate poate fi acţionat în instanţă, de către aceasta din urmă, cu o acţiune pentru apărarea şi restaurarea dreptului său încălcat[54] şi/sau cu o acţiune în despăgubire[55].

---

53 A se vedea website-ul Comisiei Europene la adresa: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/.

54 Conform art. 79 din Regulamentul (UE) 2016/679; A se vedea C.T. Ungureanu, *Legal Remedies for Personal Data Protection in European Union* în Logos Universality Mentality Education Novelty: Law, Volume 6, Issue 2, 2018, https://doi.org/10.18662/lumenlaw/10, p. 38.

55 Conform art. 82 din Regulamentul (UE) 2016/679.

4. Informaţiile publice şi activităţile de Competitive Intelligence

Informaţiile publice reprezintă o sursă de informare vitală în contextul desfăşurării activităţilor economice întrucât acestea influenţează direct cererea şi oferta, comportamentul consumatorilor şi deciziile de business. De exemplu, informaţia potrivit căreia un produs farmaceutic este disponibil în cadrul unui singur lanţ de farmacii determină migraţia consumatorilor ţintă. În aceeaşi măsură, informaţia potrivit căreia în judeţul Iaşi va fi organizat un festival internaţional de muzică poate determina creşterea tarifelor hoteliere în perioada respectivă, deschiderea unor noi afaceri în proximitatea zonei unde se desfăşoară festivalul etc. Apreciem că „informaţiile publice" reprezintă orice informaţii sau date care au fost divulgate către public şi sunt accesibile acestuia. Astfel, informaţiile publice pot fi accesate şi utilizate de orice profesionist în vederea dezvoltării şi adaptării afacerii la condiţiile pieţei însă nu pot fi considerate de către acesta din urmă drept informaţii confidenţiale sau clasificate drept secrete de serviciu.

În situaţia în care informaţiile confidenţiale sunt colectate şi prelucrate în cadrul unor activităţi de tip *Competitive intelligence*, rezultatele obţinute pot fi considerate informaţii confidenţiale sau, de ce nu, secrete de serviciu. *Competitive intelligence* desemnează procesul analitic care transformă informaţiile fragmentate despre concurenţi şi clienţi în cunoştinţe strategice relevante, precise şi utilizabile despre evoluţia pieţei, oportunităţile de afaceri şi ameninţările probabile[56].

Activităţile de *Competitive Intelligence* implică colectarea, selecţia şi interpretarea informaţiilor obţinute din surse publice, care privesc poziţia, performanţa, capacităţile şi intenţiile organizaţiilor concurente[57].

Concluzii

Plecând de la aforismul „*scientia potentia est*" („*cunoaşterea înseamnă putere*"), considerăm că accesul la informaţii nu mai prezintă nicio barieră, inclusiv cea lingvistică, fiind eliminată de către instrumentele disponibile. Liberul acces la informaţii determină pentru profesionişti şi pentru consumatori probleme în identificarea informaţiilor veridice şi, în acelaşi timp, riscuri cu privire securitatea propriilor date. În acest context, mediul de afaceri trebuie să manifeste o atenţie sporită asupra modului în care protejează informaţiile valoroase organizaţiei.

Apreciem că la baza protecţiei informaţiilor confidenţiale, a celor clasificate sau a datelor cu caracter personal ar trebui să se afle principiul "*need to know*"

---

[56] F. Albescu, I. Pugna, D. Paraschiv, *Business Competitive Intelligence – The Ultimate Use of Information Technologies in Strategic Management* în 4th International Conference of ASECU "Development Cooperation and Competitiveness" The Bucharest Academy of Economic Studies, 22-24 May 2008, Bucharest, Romania, [Online], consultat în 15.04.2020, http://www.asecu.gr/files/RomaniaProceedings/01.pdf.

[57] *Ibidem.*

care stabileşte că dreptul de a accesa o informaţie trebuie să îl aibă doar persoanele care au nevoie de respectiva informaţie în desfăşurarea atribuţiilor de serviciu. Prin respectarea strictă a acestui principiu, informaţia sensibilă va fi accesată doar de către un număr limitat de persoane, determinând astfel un control asupra modului în care sunt gestionate informaţiile şi, indirect, o responsabilizare a celui care utilizează informaţia confidenţială.

Dacă ne raportăm la conceptele analizate, considerăm că informaţiile clasificate şi datele cu caracter personal pot fi incluse în noţiunea mai „cuprinzătoare" de informaţii confidenţiale, obligaţia de a le proteja confidenţialitatea şi integritatea fiind elementul esenţial comun al acestora. Astfel, toate regulile şi principiile aplicabile informaţiilor confidenţiale se pot extinde asupra informaţiilor clasificate şi datelor cu caracter personal, la care se adaugă regulile speciale aplicabile acestor categorii speciale de informaţii.

Conchidem prin a afirma că informaţiile reprezintă unele dintre cele mai valoroase şi mai dificil de protejat active din cadrul unei afaceri. Internaţionalizarea afacerilor şi digitalizarea treptată a tuturor activităţilor determină societăţile să aloce resurse pentru protejarea informaţiilor confidenţiale şi pentru conformarea la reglementările din domeniul informaţiilor clasificate şi a datelor cu caracter personal.