ONLINE INSURANCE, CYBER RISKS AND THEIR PREVENTION

ASIGURĂRILE ONLINE, RISCURILE CIBERNETICE ȘI PREVENIREA ACESTORA

Dogotari Ilie
Doctorand, Universitatea Liberă Internațională din Moldova
e-mail: dogotari@gmail.com

Spînu Ana
Doctor în științe economice, conferențiar universitar
Universitatea Liberă Internațională din Moldova
e-mail: aspinu@ulim.md

Abstract
The actuality of the subject is explained by the fact that electronic insurance is not a future related field. Customers want electronic insurance because it has great benefits for modern people. The digital age creates many new opportunities for the economy and society. But at the same time, it brings new challenges. To have successful online insurance, insurance companies need to have a cyber risk prevention policy, so the security of networks and information systems is essential for the proper functioning of the insurance market. The aim of the research is to identify how the cyber risks influencing online insurance can be predicted. The main research methods applied to the elaboration of the article are induction, deduction, analysis, synthesis, documentation and observation. As a result of the research, we mention that to minimize the effects of cyber risks on the field of insurance, it is necessary to adopt a wide range of measures to protect the digital market and to protect infrastructure and citizens.

Keywords: *Insurance, cyber risks, online insurance, regulations, cyber security*

JEL Classification: *G220 Insurance; Insurance Companies; Actuarial Studies*

INTRODUCERE

Asigurările electronice nu mai țin de domeniul viitorului. Clienții vor asigurări electronice, pentru că ele prezintă avantaje enorme pentru omul contemporan. Azi nu mai avem timp să ne deplasăm pentru a primi un produs sau serviciu, fie el și unul financiar. Indiferent de complexitatea serviciilor, majoritatea oamenilor prefera ca acestea să fie accesibile direct din computerul său, smartphone sau tabletă.

Asemenea altor sectoare financiare, în ultimii ani se constată o creștere spectaculoasă a sectorului (industria) asigurărilor. Pe lângă mijloacele tradiționale de încheiere a polițelor de asigurare, marile companii prezente pe piață încep să acorde o importanță tot mai mare canalelor de distribuție online a produselor. Astfel, orientarea către un nou mod de promovare/vânzare a produselor va determina pe de o parte creșteri ale cifrei de afaceri a companiilor de asigurări, în timp ce pe de altă parte, ia amploarea, frecvența și impactul incidentelor de securitate care sunt în creștere și reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Sistemele respective pot să devină, de asemenea, o țintă pentru acțiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcționarea sistemelor. Astfel de incidente pot să împiedice desfășurarea activităților economice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore companiei.

REZULTATELE CERCETĂRII

Era digitală creează numeroase noi oportunități pentru economie și societate. Dar, în același timp, introduce noi provocări. Un studiu privind atitudinile față de securitatea cibernetică efectuat de Eurobarometru în 2018 arată că cetățenii UE sunt preocupați de securitatea cibernetică și de confidențialitate [18]. Astfel, 88% dintre utilizatorii zilnici de internet și-au exprimat mari îngrijorări cu privire la atacurilor cibernetice, iar 77% dintre utilizatorii zilnici de internet și-au exprimat mari îngrijorări cu privire la faptul că informațiile lor personale nu sunt păstrate în siguranță de site-uri web.

Pentru ca asigurările online să aibă succes este necesar ca companiile de asigurare să aibă o politică de prevenire a riscurilor cibernetice, prin urmare, securitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței de asigurări.

Asigurarea electronică reprezintă totalitatea documentelor electronice ce constituie actul juridic prin care asiguratul se obligă să plătească o primă asiguratorului care preia asupra sa riscul asigurat, obligându-se la producerea acestuia, să plătească asiguratului sau unei terțe persoane o despăgubire sau suma asigurată.

Dezvoltarea tehnologiei informaționale din ultimii ani, a dus la schimbarea radicală a mediului de afaceri. Deschiderea info-structurii IP (Internet Provider) a înlesnit apariția noilor modele de afaceri și a creat oportunități fenomenale.

Tot mai multe întreprinderi își trec afacerile pe online, în special comerțul, deoarece acesta implică mai puține costuri, astfel fiind mai profitabile. Însă, odată cu începerea activităților pe online, apar o mulțime de probleme, precum:

- veridicitatea informațiilor;
- imposibilitatea interzicerii intrării persoanelor nedorite în rețea;
- securitatea datelor clienților.

Se presupune că o afacere online creează medii nesigure de lucru. În acest sens, trebuie evaluate riscurile și beneficiile pe care o societate le are în urma implementării IT și, în funcție de acestea trebuie organizată activitatea pe care o desfășoară.

În discursul său despre statul Uniunii de pe 13 septembrie 2017[15], președintele Comisiei Europene, Jean-Claude Juncker a menționat că *atacurile cibernetice nu cunosc frontiere și nimeni nu este imun.*

Noțiunea de risc cibernetic cuprinde o multitudine de riscuri care amenință bunurile firmelor, guvernelor sau persoanelor fizice, pierderile în general incluzând active financiare sau nefinanciare, identități, divulgarea de informații sensibile și întreruperea activităților/afacerii.

Conform statisticii guvernului Regatului Unit, criminalitatea informatică generează pierderi anuale de peste 38 miliarde USD [5]. Chiar și așa, în Europa 68% dintre organizații nici nu au estimat impactul financiar al unui atac cibernetic. Doar 25% dintre companii dețin un plan de răspuns în cazul atacurilor cibernetice. La nivel mondial, se estimează pierderi cauzate de riscuri cibernetice la aproape 0,5% din PIB-ul mondial și aproape de două ori mai mult decât media anuală a pierderilor datorate dezastrelor naturale.

Se estimează că riscurile aferente activității în mediul online, apar de fiecare dată când se deschide o poartă în rețea, de fiecare dată când se permite accesul unei persoane din exterior la rețeaua companiei. Afacerile online reprezintă o activitate nouă și majoritatea companiilor nu realizează riscurile aferente acestui nou format. Printre acestea se enumeră:

- responsabilitatea companiei pentru datele colectate, utilizate și stocate, de la clienți, parteneri și angajați;

- pierderea datelor personale sau ale clienților - o amenințare constanta pentru orice companie - exista riscul unui atac de tip hacking sau a unor incidente interne, ca urmare a neglijenței sau unui act intenționat;
- pierderea de venituri ca urmare a întreruperii activități;
- riscuri reputaționale;
- riscuri de atac în scopul răscumpărărilor;
- riscul de sancțiuni din partea supraveghetorilor

Riscul cibernetic trebuie gestionat din mai multe perspective. Modelul clasic de gestionare a riscului cibernetic cuprinde următoarele etape:

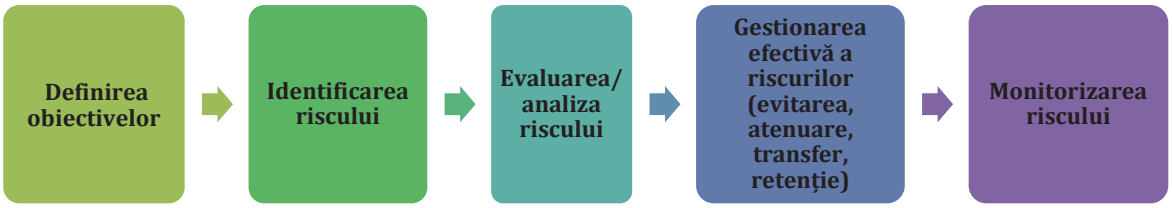

Figura 1. Etapele de gestionare a riscului cibernetic

Sursa: [elaborat de autor]

Pentru ca asigurările online să se dezvolte, trebuie excluse sau, cel puțin, minimizate riscurile cibernetice. Toți emitenții de asigurări online trebuie să garanteze consumatorului/clientului un mediu sigur.

Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare. În acest sens, asiguratorii trebuie să adopte politici interne și să pună în aplicare măsuri care să respecte, în special, principiul protecției implicite a datelor, în corespundere cu legislația privind protecția datelor cu caracter personal.

Uniunea Europeană a adoptat o gamă largă de măsuri pentru a proteja piața unică digitală europeană și pentru a proteja infrastructura, guvernele, întreprinderile și cetățenii. Printre aceste măsuri se enumeră și un șir de reglementări.

Unul dintre aceste acte este *Regulamentul general privind protecția datelor (GDPR)* [16] - introdus în mai 2018, care oferă noi reguli pentru a oferi cetățenilor un control mai mare asupra datelor lor personale și un avantaj competitiv pentru companiile conforme.

Un alt document este *Directiva privind confidențialitatea electronică* [17], care asigură protejarea confidențialității comunicărilor noastre online. Această directivă asigură confidențialitatea comunicărilor și definește regulile privind urmărirea și monitorizarea online. La momentul actual directiva urmează a fi actualizează pentru a acoperi noile mijloace de comunicații online, astfel de e-mailuri web și servicii de mesagerie (Regulamentul ePrivacy).

Drept exemplu mai poate fi adus și *Regulamentul eIDAS* [18], document ce reglementează sistemul de identificare și autentificare electronică la nivelul UE. Sistemul de identificare electronică, autentificare și servicii de încredere (eIDAS) a intrat în vigoare în octombrie 2018, introducând modalități sigure pentru persoanele fizice și companiile de a efectua tranzacții online.

Acest sistem include:

- ✓ Un sistem de semnături digitale transfrontaliere;
- ✓ Profilare digitală conformă cu GDPR;
- ✓ Respectarea principiului „o singură dată”, în care cetățenii și companiile trebuie să furnizeze autorității informații standard o singură dată.

Deci, în scopul dezvoltării unui mediu sigur este necesar ca autoritățile de supraveghere și control să creeze reguli clare și stricte în ceea ce privește siguranța informațională.

Dreptul la viață privată este expres prevăzut în Constituția Republicii Moldova, prin consacrarea sa în Articolul 28, care prevede că "statul respectă și ocrotește viața intimă, familială și privată" care include în sine și dreptul la protecția datelor cu caracter personal. La 15 februarie 2007 a fost aprobată prima lege privind protecția datelor cu caracter personal [19], acel act legislativ definea domeniul de aplicare, noțiunile principale și cerințele de bază în procesul de prelucrare a datelor cu caracter personal, stabilind regimul de confidențialitate și instituirea Centrului Național pentru Protecția Datelor cu Caracter Personal ca autoritate de supraveghere și control. Ulterior, pe data de 8 iulie 2011 a fost adoptată Legea Nr. 133[7] privind protecția datelor cu caracter personal în versiune nouă, fapt ce a permis eliminarea, în mare parte, a discrepanțelor între legislația europeană și cea națională. Deși de la adoptarea noii legi privind protecția datelor cu caracter personal a trecut o perioadă, constatăm, totuși, un șir de restanțe în ceea ce privește implementarea ei.

Concepţia securităţii informaționale a Republicii Moldova, aprobată prin Legea nr. 299/2017, reprezintă documentul de bază pentru elaborarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024. Aceasta strategie urmează să transpună la nivel național modelul european de dezvoltare a societății informaționale și a poate fi considerată un punct de pornire pentru consolidarea protejării intereselor persoanelor, ale societăţii și ale statului în domeniul informaţional.

Pe lângă Centrul Național de Protecție a Datelor cu Caracter Personal, este necesar ca și Comisia Națională a Pieței Financiară să elaboreze politici și regulamente care să vizeze securitatea informațională a clienților pe piața asigurărilor. În România, de exemplu, există deja Ghidul Consumatorului privind Comercializarea prin Mijloace electronice a produselor și serviciilor de Asigurare. În acestea sunt explicate clienților noțiunile de bază. Totodată, sunt explicate drepturile și obligațiunile asiguraților. De asemenea, sunt enumerate un șir de cerințe ce trebuie să le întrunească o pagină destinată comerțului online, astfel încât, clientul să aibă măcar câteva criterii la care ar putea să facă referire atunci când decide să procure o asigurare electronică [4]. Toate aceste lucruri, conferă entităților emitente de servicii electronice, în primul rând mai multă credibilitate și în al doilea rând, acestea sunt obligate să întrunească norme minime de siguranță.

Piața de asigurări din România, a fost nevoită să treacă printr-o serie de schimbări legislative. Printre acestea, se numără ajustarea cadrului legal cu Regulamentul privind Protecția Datelor Personale (GDPR), și Directiva privind Distribuția în Asigurări (IDD) – care a transformat întreaga distribuție de asigurări, a pus accent pe protecția consumatorilor și impune o serie de cerințe exigente în ceea ce privește pregătirea profesională.

Companiile de pe piața de asigurări din România, au înţeles foarte bine răspunderea adusă de noul regulament privind protecţia datelor şi au reacţionat prompt pentru implementarea cerinţelor legislative, unii începând introducerea prevederii chiar din 2017. Companiile din industria asigurărilor au reuşit să integreze cu succes prevederile GDPR în fluxul intern de lucru, sporind astfel încrederea clienţilor şi câştigând valoare adăugată prin prelucrarea securizată a datelor cu caracter personal.

Pe lângă acestea, în România au fost elaborate un șir de acte normative care au menirea să protejeze asiguraţii și să constrângă brokerii și asigurătorii să se conformeze cerințelor vis-a-vis siguranța informațională, precum:

1. *Norma nr.15/2015 privind comercializarea prin mijloace electronice a contractelor de asigurare [2]* care stabilește condițiile în baza cărora Autoritatea de Supraveghere Financiară (ASF) reglementează activitatea de comercializare prin mijloace

electronice a contractelor de asigurare. Norma a impus un minim necesar de condiții pentru furnizori de soluții și/sau aplicații software dedicate pentru activitatea de comercializare on-line sau prin mijloace electronice a contractelor de asigurare - care include prezentare informației despre serviciilor oferite către utilizator, politica de prelucrare a datelor cu caracter personal și securitate cu obligativitatea utilizării protocolului de securitate Transport Layer Security (TLS utilizând chei de minimum 2048 biti), sau protocoale similare ori cu aceleași capacități tehnice și certificate emise de un furnizor acreditat.

Această normă a fost valabilă până la 20 decembrie 2018, fiind abrogat și înlocuită prin *Norma 19/2018 privind distribuția de asigurări* care reglementează: încadrarea intermediarilor de asigurări, reasigurări și asigurări auxiliare în anumite categorii, raporturile juridice dintre distribuitori și canalele de distribuție ale acestora, procesul de înregistrare a intermediarilor, procesul de supraveghere și monitorizare permanentă de către ASF - Autoritatea de Supraveghere Financiară a activității de distribuție desfășurate de către distribuitori, inclusiv a respectării regulilor de conduită, activitatea de comercializare a contractelor de asigurare prin intermediul site-urilor distribuitorilor și/sau prin alte mijloace de comunicare, etc.

2. Ordinul CSA nr. 23/2009 pentru punerea în aplicare a Normelor privind informațiile pe care asigurătorii și intermediarii în asigurări trebuie să le furnizeze clienților [3]. Această normă a fost valabilă până la 20 decembrie 2018, fiind abrogată prin Normă 19/2018 privind distribuția de asigurări menționată anterior.

Spre deosebire de alte industrii, companiile din domeniul asigurărilor prelucrează o gamă largă de date cu caracter personal pentru scopuri diverse, precum servicii de asigurare de viaţă, asigurare de sănătate, soluţionarea dosarelor de daună şi altele. Astfel, protecția datelor este esențială pentru menținerea încrederii asiguraților.

Prin exemplele menționate ne convingem de faptul că cadrul normativ în domeniul protecției asiguraților și activității intermediarilor de asigurări și asigurătorilor este în continuă modificare și perfectare.

Deși, în Legislația Republicii Moldova sunt norme care reglementează securitatea informațională, protejarea datelor cu caracter personal, printre care regăsim și Legea privind protecţia datelor cu caracter personal scopul căreia este asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale şi private [7], acestea totuși, din dorința de a cuprinde toate domeniile existente sunt mult prea generale, iar pe alocuri neclare pentru domenii anume. Din acest motiv, este necesar ca autoritățile de supraveghere să conlucreze, astfel încât companiile de asigurare și brokerii să aibă norme clare, regulamente de care se pot conduce în procesul de lucru. Ideal ar fi ca autoritățile să organizeze seminarii de instruire, care să finalizeze cu examene.

Totodată, pe lângă cerințele legale vis-a-vis de siguranța datelor, este important ca fiecare companie, dar mai ales, emitenții de servicii electronice de asigurare, să implementeze standardelor internaționale de management al securității informaționale, ISO 27001, acesta demonstrează angajamentul pentru protecţia datelor procesate, continuitatea activităţilor (business continuity) şi respectarea legislaţiei naţionale şi internaţionale în domeniu [1].

Alinierea la Cadrul UE de certificare de securitate cibernetică ar aduce avantaje întregului sistem al asigurărilor. Sistemul european de certificare de securitate cibernetică este un set cuprinzător de norme, cerințe tehnice, standarde și proceduri convenite la nivel european pentru evaluarea proprietăților de securitate cibernetică ale unui anumit produs, serviciu sau proces.

Certificarea de securitate cibernetică joacă un rol important în sporirea încrederii utilizatorilor în produsele, serviciile și procesele care sunt esențiale pentru funcționarea corespunzătoare a pieței unice digitale și în consolidarea securității acestora. Având în vedere gama largă de produse, servicii și procese TIC și multiplele întrebuințări date acestora, cadrul european de certificare de securitate cibernetică permite crearea unor sisteme UE de certificare personalizate și bazate pe riscuri.

Pentru a exprima riscul de securitate cibernetică, un certificat se poate referi la trei niveluri de asigurare (de bază, substanțial, ridicat), care sunt proporționale cu nivelul de risc asociat utilizării preconizate a produsului, procesului sau serviciului în cauză din perspectiva probabilității survenirii unui incident și a impactului acestuia. De exemplu, un nivel ridicat de asigurare înseamnă că produsul care a fost certificat a trecut cele mai exigente teste de securitate.

Certificatul acordat va fi recunoscut în toate statele alineate la cadrul UE, ceea ce va facilita, pe de o parte, schimburile comerciale transfrontaliere între întreprinderi și, pe de altă parte, înțelegerea de către utilizatori a elementelor de securitate ale produsului sau serviciului respectiv. Acest lucru permite o concurență benefică între furnizori pe întreaga piață a UE, ceea ce se reflectă într-o mai bună calitate a produselor și într-un raport calitate-preț mai bun.

Consumatorii au dreptul de a primi informații corecte, încă înainte de a încheia un contract de asigurare, adică în faza precontractuală, referitor la toate condițiile contractului de asigurare.

Este important ca persoana să înțeleagă de ce anumite categorii de date sunt colectate, o pagină de internet care comercializează produse de asigurare online, trebuie să dea explicații clar clienților săi, de ce unele date sunt colectate și de ce anume într-o anumită măsură. Până la procurarea produsului de asigurare, clientul trebuie să facă cunoștință cu termenii și condițiile companiei, cu politica de confidențialitate, cu regulile ce țin de reziliere, returnarea de primă și calculul primei de asigurare.

Conținutul paginii de internet trebuie să fie unul accesibil, clar, fără echivoc, nu trebuie să fie solicitată informație suplimentare, ce ar putea fi utilizate în scopuri decât emiterea contractelor de asigurare. Este foarte important ca utilizatorul paginii să-și dea consimțământul pentru prelucrarea datelor cu caracter personal, și nu doar! Clientul trebuie să aibă opțiunea de a alege scopurile pentru care pot fi utilizate acele date.

Dar până a ajunge la acest nivel, este necesară educarea populației. Mare parte a populației din Republica Moldova suferă de lipsă de cunoștințe în domeniul juridic și financiar. Cum ar putea persoana să fie pregătită să procure ceva online, nemaivorbind de asigurări electronice, dacă aceștia nu înțeleg, sau ce e mai grav, nu au acces la internet, la un card. Este de datoria statului să informeze populația despre modul în care populația își poate gestiona riscurile. Aceste lucruri trebuie educate din școli, la cea mai fragedă vârstă. După care am putea să ne racordăm la cele mai variate studii din Europa, și să preluăm practicile acestora. Moldovenii în continuare preferă să facă cumpărături offline. Mai ales când vorbim despre produsele financiare, precum asigurările.

Drept argument a celor menționate apelăm la raportul BNM referitor la indicatorii activității în cadrul sistemelor de plăți cu cardurile de plată din Republica Moldova pentru anul 2019 [12] conform căruia se constată că din volumul total al operațiunilor cu carduri de 70 594 184,5 mii lei doar 4 471 477,25 mii lei sunt plăți fără numerar fără prezența fizică a cardului cea ce constituie o cotă de 6,33%. Astfel, se observă o lipsa de încredere din partea populației față de tot ce ține de comerțul electronic.

CONCLUZII

În concluzie constatăm că în vederea dezvoltării asigurărilor online trebuie excluse sau, cel puțin, minimizate riscurile cibernetice. În acest scop este necesar de a actualiza legislația Republicii Moldova care este alcătuită din norme mult prea generale, iar pe alocuri neclare pentru domenii anume. Din acest motiv, este necesar ca autoritățile de supraveghere să conlucreze, astfel încât companiile de asigurare și brokerii să aibă norme clare, regulamente de care se pot conduce în procesul de lucru.

BIBLIOGRAFIE

1. ISO/IEC 27001. Information security management. Disponibil: http://www.iso.org/isoiec-27001-information-security.html
2. Norma nr.15/2015 privind comercializarea prin mijloace electronice a contractelor de asigurare. În: Monitorul Oficial al României, Partea I nr. 641 din 24 august 2015. Disponibil: https://lege5.ro/Gratuit/g42tenbvg4/norma-nr-15-2015-privind-comercializarea-prin-mijloace-electronice-a-contractelor-de-asigurare
3. Ordinul nr. 23/2009 pentru punerea în aplicare a Normelor privind informațiile pe care asigurătorii și intermediarii în asigurări trebuie să le furnizeze clienților, precum și alte elemente pe care trebuie să le cuprindă contractul de asigurare. În: Monitorul Oficial al României, Partea I nr. 908 din 23 decembrie 2009. Disponibil: http://lege5.ro/Gratuit/geztaobygy/ordinul-nr-23-2009-pentru-punerea-in-aplicare-a-normelor-privind-informatiile-pe-care-asiguratorii-si-intermediarii-in-asigurari-trebuie-sa-le-furnizeze-clientilor-precum-si-alte-elemente-pe-care-treb
4. ASF. Ghidul Consumatorului privind Comercializarea prin Mijloace electronice a produselor și serviciilor de Asigurare. Disponibil: http://asfromania.ro/files/consumatori/Ghid_comert%20electronic.pdf
5. Cyber Essentials: Requirements for IT infrastructure. Disponibil: http://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf
6. Geneva Association. Understanding and Addressing Global Insurance Protection Gaps. Disponibil: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf
7. LEGE Nr. 133din 08-07-2011 privind protecţia datelor cu caracter personal. În: Monitorul Oficial al RM, Nr. 170-175 art.492. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110544&lang=ro
8. Directiva privind securitatea rețelelor și a sistemelor informatice. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
9. Legea UE privind securitatea cibernetică . Disponibil: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
10. Noile norme în domeniul telecomunicațiilor intră în vigoare. http://ec.europa.eu/commission/presscorner/detail/ro/IP_09_1966
11. Legea Nr. 299 din 21-12-2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova. Disponibil: http://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
12. Raport: Indicatorii activităţii în cadrul sistemelor de plăţi cu cardurile de plată din Republica Moldova. Disponibil: http://www.bnm.md/bdi/pages/reports/dsp/DSP1.xhtml?id=0&lang=ro
13. Eurobarometru. Europa pentru cetățeni. http://www.europarl.europa.eu/romania/ro/ue_pentru_celateni/eurobarometru.html
14. Norma 19/2018 privind distribuția de asigurări. Disponibil: https://asfromania.ro/files/Asigurari/norme/2019/Norma%2019_2018%20%20%20_MoF.pdf
15. Discursul Președintelui JEAN-CLAUDE JUNCKER PRIVIND Starea Uniunii 2017. Disponibil: http://ec.europa.eu/commission/presscorner/detail/ro/SPEECH_17_3165

16. Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
17. 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. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=RO
18. Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32014R0910&from=RO
19. LEGE Nr. 17 cu privire la protecţia datelor cu caracter personal din 15.02.2007. Disponibil: http://lex.justice.md/index.php?action=view&view=doc&lan-g=1&id=324657